Poznámky z přednášek
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

Vybrané kapitoly z výpočetní složitosti I (samoopravné kódy)

Peter Černo, 2011
petercerno@gmail.com

Garant: Mgr. Michal Koucký Ph.D.
E-mail: Michal.Koucky@mff.cuni.cz
Domácí stránka: `http://www.math.cas.cz/~koucky/`

Anotace: Obsahem této přednášky jsou pokročilé partie z výpočetní složitosti. Každý semestr bude věnován jinému tématu. Mezi plánovaná témata patří oblast náhodnosti a pseudonáhodných generátorů, komunikační složitost a interaktivní protokoly, samoopravné kódy a jejich užití ve složitosti, dolní odhady, expandery a jejich použití a další. Přednáška je určena především studentům vyšších ročníků studia a doktorandům. Přednáška předpokládá základní znalosti z výpočetní složitosti, pravděpodobnosti a diskrétní matematiky.

Sylabus:

1. Náhodnost a pseudonáhodné generátory.
2. Komunikační složitost a interaktivní protokoly.
3. Samoopravné kódy.
4. Dolní odhady.
5. Expandery a jejich použití.

Literatura:

1. Sanjeev Arora and Boaz Barak: Computational Complexity: A Modern Approach (`http://www.cs.princeton.edu/theory/complexity/`)

Vybrané kapitoly z výpočetní složitosti I

Michal Koucký
<koucky@math.cas.cz>

ZS 2010/2011

TIN085 - 2/1 Z, Zk

Čas konání: pátek 12:20-13:50.
Místo konání: S4 - Malá Strana

Obsahem této přednášky jsou pokročilé partie z výpočetní složitosti. Tento semestr bude věnován samoopravným kódům. Samoopravné kódy jsou kombinatorický objekt s fascinujícími vlastnostmi. Na přednášce se budeme zabývat základními vlastnostmi samoopravných kódů, jejich konstrukcí a užitím ve složitosti. Ukážeme jak některé algebraické konstrukce tak konstrukce kombinatorické. I když toto téma může vypadat jako čistě teoretické, bez této teorie by nefungovaly CD-přehrávače, mobily, moderní procesory, paměti, pevné disky, zkrátka žádné zařízení skladující nebo přenášející data. Význam samoopravných kódů pro praktické aplikace neustále roste a tudíž lze tuto přednášku doporučit nejen zájemcům o teorii.

Přednáška je určena především studentům vyšších ročníků studia a doktorandům. Přednáška předpokládá základní znalosti z diskrétní matematiky, algebry, pravděpodobnosti a výpočetní složitosti.

Plán přednášky

- Shannonův a Hammingův přístup.
- Náhodné kódy, Hadamardovy, Hammingovy, Reed-Solomonovy kódy.
- Dekódování RS kódů (algoritmus Berlekampa a Welshe).
- Dekódování s více možnostmi.
- Skládání kódů.
- Reed-Mullerovy kódy.
- Kód Sipsera a Spielmena.
- Lokálně dekódovatelné kódy.
- Užití.
- Kombinatorická omezení kódů.

Literatura:

F.J. MacWilliams and N.J.A. Sloane: **The Theory of Error Correcting Codes.** North-Holland, Amsterdam, 1981.
Madhu Sudan – lecture notes.

08.10.2010 Fr
PETER ČERNO

NTIN085 Vybrané kapitoly z výp. složnosti I

Samoopravné kódy

MICHAL KOUCKÝ

ZÁPOČET ... 4 SADY DOMÁCICH ÚLOH
TREBA VYRIEŠIŤ ASPOŇ 50%

LECTURE NOTES MADHU SUDAN

ADÁMEK - KÓDOVÁNÍ

ALGEBRA ... POTREBUJEME KONEČNÉ TELESÁ
PRAVDEPODOBNOSŤ ... ZÁKLADNÉ VECI

KÓDY - ČO TO SÚ, K ČOMU SÚ

REED-SOLOMONOVÉ KÓDY
REED-MÜLEROVE KÓDY
} ALGEBRAICKÉ KÓDY

GALLAGEROVE KÓDY
SPIELMAN-SIPSER KÓDY
SPIELMANOVÉ KÓDY
} KOMBINATORICKÉ KÓDY

RAPTOR KÓDY ... ŠPECIÁLNE KÓDY

$x \in \{0,1\}^k \longrightarrow x' \in \{0,1\}^k$

$101101 \longrightarrow 110101$

RÔZNE PRÍPADY: KOMUNIKÁCIA PO SIETI
ZÁPIS NA DISK

- KAŽDÝ BIT POSLEM 3x

111000111111000111 → DOŠLO K 1 CHYBE

→ 111010111111000111 ← VŽDY VEZMEM MAJ

1 0 1 1 0 1

TOTO RIEŠENIE JE SCHOPNÉ OPRAVIŤ VO VŠEOBECNOSTI MAXIMÁLNE 1 CHYBU

DOKÁŽE DETEKOVAŤ 2 CHYBY.

VÝHODA RIEŠENIA ... DOKÁŽE OPRAVIŤ 1 CHYBU
NEVÝHODA RIEŠENIA ... POTREBUJE 3k BITOV

PRI POUŽITÍ 5 BITOV ...
VIEM OPRAVIŤ 2 CHYBY
DETEKOVAŤ 4 CHYBY

HAMMINGOV KÓD

$k = 4 \longrightarrow n = 7$

POPIS POMOCOU TZV. GENERUJÚCEJ MATICE

$$G_{HAM} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

08.10.2010 Fr
PETER ČERNO

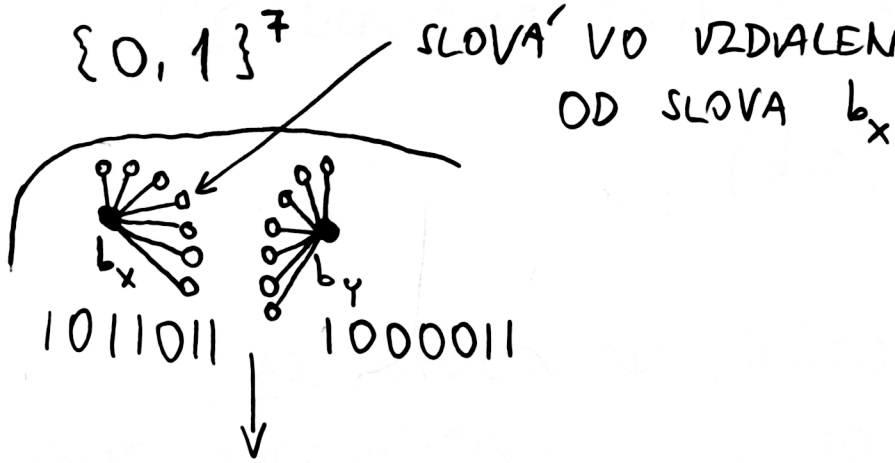
NTINO85 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

$$(x_1, x_2, x_3, x_4) \longrightarrow (x_1, x_2, x_3, x_4) \cdot G = b$$

<u>NAD TELESOM</u> $GF[2]$ ... TJ. $\mathbb{Z} \bmod 2$

<u>VETA</u>: $\forall x, y \in \{0,1\}^4,\ x \neq y$
$\Rightarrow$ $x \cdot G$ A $y \cdot G$ SA LÍŠIA ASPOŇ NA TROCH POZÍCIACH.

OZNAČME $b_x = x \cdot G$, $b_y = y \cdot G$



DÔSLEDOK VYŠŠIE UVEDENÉHO TVRDENIA: TIETO MNOŽINY SÚ RÔZNE

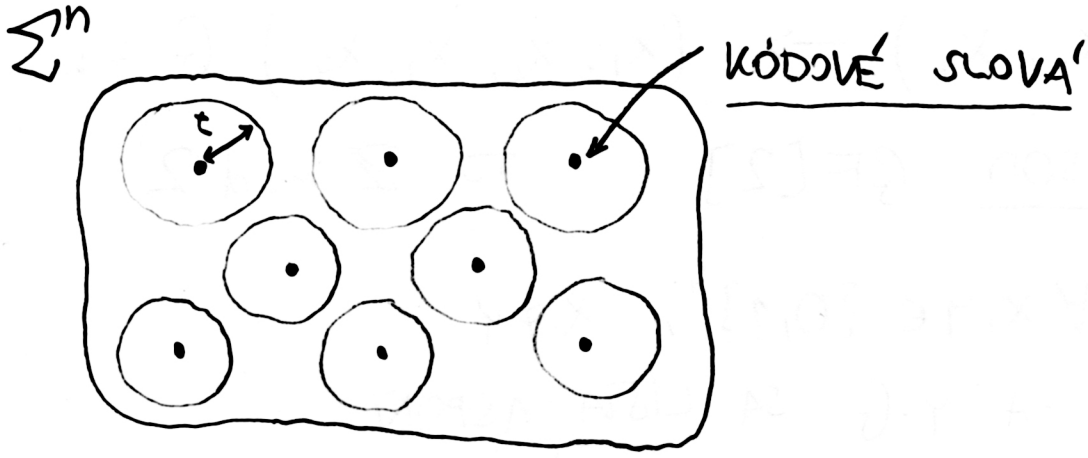
$\Rightarrow$ <u>HAMMINGOV KÓD</u> OPRAVUJE 1 CHYBU DETEKUJE 2 CHYBY.

<u>TERMINOLÓGIA</u>: <u>KÓD</u> JE $C \subseteq \{0,1\}^7$

$$C = \{ x \cdot G \mid x \in \{0,1\}^4 \}$$

<u>KÓDOVÉ SLOVO</u> ↑ ↑ <u>SPRÁVA</u>

KONVENCIA : k ... DĹŽKA SPRÁV
n ... DĹŽKA KÓDU



POKIAĽ JE VZDIALENOSŤ KÓDOVÝCH SLOV $\geq 2t+1$
$\Leftrightarrow$ VIEM OPRAVIŤ (DETEKOVAŤ) t $(2t)$ CHÝB.

PERFEKTNÝ KÓD $\equiv$ GUĽE POKRÝVAJÚ Σ^n

$$\Delta(C) = \min_{\substack{a,b \in C \\ a \neq b}} \Delta(a,b)$$

$\Delta(a,b)$ = # POZÍCIÍ, NA KTORÝCH SA a LÍŠI OD b ... HAMMINGOVA VZDIAL.

Δ(HAMMINGOVHO KÓDU $4 \to 7$) = 3

KONVENCIA : d ... MINIMÁLNA VZDIAL. KÓDOV
q ... VELKOSŤ ABECEDY

$\frac{d-1}{2}$ ... # CHÝB, KT. VIEM OPRAVIŤ

HAMMINGOV KÓD ... $(n,k,d)_q = (7,4,3)_2$.

08.10.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

- CHCEME, ABY d RASTLO LINEÁRNE S n ...

MOTIVÁCIA : OČAKÁVANÝ POČET CHÝB RASTIE LINEÁRNE S POČTOM BLOKOV

- TAKMER POŽADUJEME $\frac{k}{n}$ = konšt.

... LINEÁRNY OVERHEAD

POKIAĽ OČAKÁVAME V KAŽDOM BLOKU 1 CHYBU, TAK JE TO OK.

PROBLÉM : AK SÚ TIE CHYBY NEZÁVISLÉ $(p = \frac{1}{7})$

$\Rightarrow$ PRI VYSOKOM POČTE BLOKOV NASTANÚ 2 CHYBY V 1 BLOKU TAKMER ISTO !

$\Rightarrow$ MÁ ZMYSEL UVAŽOVAŤ DLHŠIE KÓDY.

DÔKAZ VETY O HAMMINGOVOM KÓDE.

LINEÁRNY KÓD :

KÓDOVÉ SLOVO + KÓD. SLOVO = KÓD. SLOVO

$$x \cdot G + y \cdot G = (x+y) \cdot G$$

LINEÁRNE KÓDY MOŽNO REPR. MATICOU...

KONTROLNÁ MATICA HAM. KÓDU $[7,4,3]_2$:

$$H = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

VEZMIME KÓDOVÉ SLOVO $b = x \cdot G$.

POTOM $b \cdot H = 0$.

PLATÍ AJ NAOPAK, TJ. AK $b \cdot H = 0 \Rightarrow b$ JE KÓDOVÉ SLOVO.

STAČÍ OVERIŤ IBA RIADKY G_i. $i = 1,2,3,4$

ZVYŠNÉ KÓDOVÉ SLOVÁ VYPLÝVAJÚ Z LINEARITY.

UVAŽUJME $x \cdot G = a$, NECH a' VZNIKNE Z a ZMENOU 2 BITOV, TJ.

$a' = a + e_i + e_j$, $i \neq j$. $\quad e_k = (0, \dots, 0, \overset{k\text{-TÝ STĽPEC}}{1}, 0, \dots, 0)$

POLOŽME $a'' = a + e_i$. POTOM $a'' \cdot H = e_i H = H_{i\cdot}$

$a' \cdot H = e_i H + e_j H = H_{i\cdot} + H_{j\cdot} \neq 0$.

$\Rightarrow$ MINIMÁLNA VZDIALENOSŤ HAM. KÓDU JE 3. $\square$

TÚTO MYŠLIENKU MOŽNO ZOVŠEOBECNIŤ:

$$H_\ell = \underbrace{\begin{pmatrix} 0 & \dots & 01 \\ 0 & \dots & 10 \\ 0 & \dots & 11 \\ & \dots & \\ 1 & \dots & 11 \end{pmatrix}}_{\ell} \Bigg\} \; 2^\ell - 1$$

DÁVA KÓD $\underline{\underline{[2^\ell - 1, 2^\ell - 1 - \ell, 3]_2}}$

$C = \{ b \in \{0,1\}^{2^\ell - 1} \mid bH = 0 \}$

$\Rightarrow G$, $\dim G = 2^\ell - 1 - \ell = k$

08.10.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

$\Rightarrow$ MÁME $[2^l-1, 2^l-1-l, 3]_2$ KÓD

$$\frac{k}{n} = \frac{2^l-1-l}{2^l-1} \to 1$$ MALÝ OVERHEAD

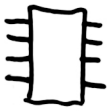
$$\frac{d}{n} = \frac{3}{2^l-1} \to 0.$$

POUŽITIE SAMOOPRAVNÝCH KÓDOV:

CD ... REED-SOLOMONOV

KOMUNIKÁCIA S DRUŽICAMI ... REED-MÜLLER

SSD

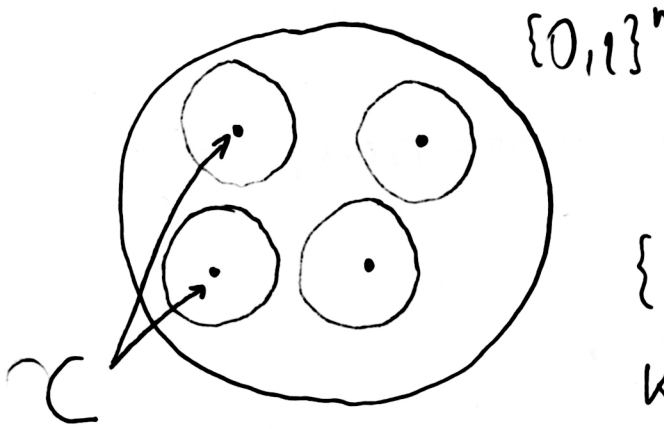


NA 512B V SÚČASNOSTI SA DÁ OPRAVIŤ 24 CHYB (ASI NIE ĽUBOVOLNÝCH, BCH KÓDY)

15.10.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

HOMEWORK ... DO 29.10.2010



$= |\{0,1\}|$

$Ball_2(x,t) =$

$\{ y \in \{0,1\}^n \mid \Delta(x,y) \leq t \}$

KDE $x \in \{0,1\}$.

CHCEME MAXIMALIZOVAŤ $|C|$ PRE DANÉ n A t.

NECH $t = pn$, p KONŠTANTA, $0 < p < 1/2$

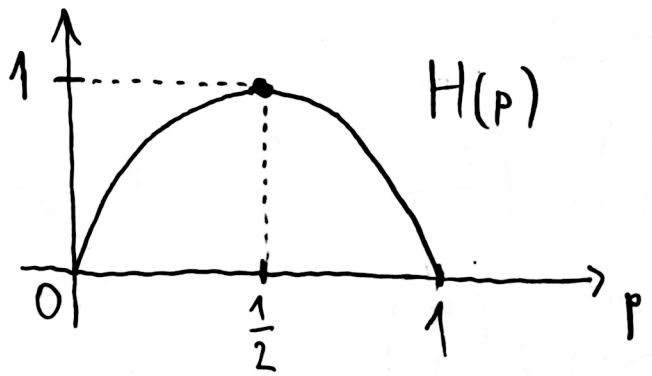
VETA: PRE $0 < p < \frac{1}{2}$:

$$\boxed{\frac{2^{nH(p)}}{n+1} \leq Vol_2(n, pn) \leq 2^{n \cdot H(p)}}$$

KDE $Vol_2(n,t) = |Ball_2(0^n, t)|$

$H(p) = -p \log_2 p - (1-p) \log_2 (1-p)$

TZV. BINÁRNA ENTROPIA (SHANNONOVA ENTR.)



HORNÝ ODHAD NA VEĽKOSŤ KÓDU JE POTOM

$$\leq \frac{2^n (n+1)}{2^{n H(p)}} \leq 2^{(1-H(p))n + \log_2 n}$$

TOTO JE DOBRÁ SPRÁVA ... TEORETICKY JE TEDA MOŽNÉ KÓDOVAŤ:

$$k \approx \underbrace{(1 - H(p))}_{\varepsilon} n \longrightarrow n$$

TJ. KÓD $(n, \varepsilon n, pn)$ $\qquad \frac{k}{n} = \frac{\varepsilon n}{n} = \text{konst.}$

$\varepsilon \approx 1 - H(p)$ $\qquad \frac{pn}{n} = p = \text{konst.}$

V PRAXI VIEME IBA $\varepsilon \ll 1 - H(p)$.

DÔKAZ TVRDENIA.

$$\mathrm{Vol}_2(n, pn) = \sum_{j=0}^{pn} \binom{n}{j} \ldots$$ TOTO CHCEME ODHADNÚŤ

$$1^n = \left(\frac{k}{n} + \frac{n-k}{n}\right)^n = \sum_{j=0}^{n} \binom{n}{j} \cdot \left(\frac{k}{n}\right)^j \left(\frac{n-k}{n}\right)^{n-j} \geq$$

$$\geq \sum_{j=0}^{k} \ldots$$ ZVOLME $k = pn$

ZREJME $\frac{k}{n} \leq \frac{1}{2}$, $\frac{n-k}{n} \geq \frac{1}{2}$

$$\left(\frac{k}{n}\right)^j \cdot \left(\frac{n-k}{n}\right)^{n-j} \geq \left(\frac{k}{n}\right)^k \cdot \left(\frac{n-k}{n}\right)^{n-k}$$ PRE $j \leq k$

$$\Rightarrow 1^n \geq \left(\frac{k}{n}\right)^k \left(\frac{n-k}{n}\right)^{n-k} \sum_{j=0}^{k} \binom{n}{j}$$

15.10.2010 Fr
PETER ČERNO

NTINO85 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI I

$$\left(\frac{k}{n}\right)^k \left(\frac{n-k}{n}\right)^{n-k} = 2^{-nH(k/n)}$$

CIEL JE DOKÁZANIE HORNÉ ODHAD.
DOLNÝ ODHAD JE ZA DOMÁCE CVIČENIE. □

HAMMING

SHANNON ... 1940, BELL LABS

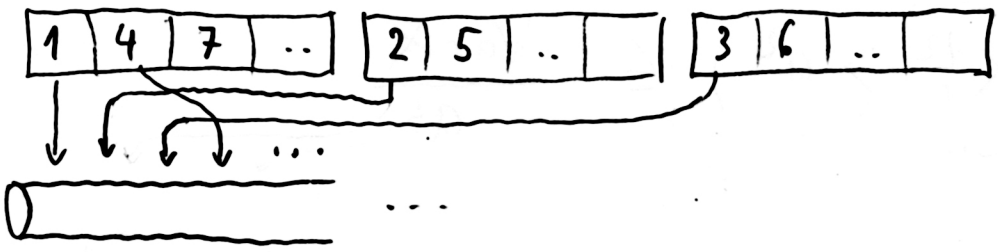
- AKO PRENÁŠAŤ SIGNÁL $m \rightsquigarrow m'$
- OKREM INÉHO SHANNON VYBUDOVAL TEÓRIU INF.

MÔŽEM PRENÁŠAŤ 0/1 ... S NEJAKOU PRAVDEPODOBNOSŤOU p DÔJDE K CHYBE
CHYBY SÚ NEZÁVISLÉ

SYMETRICKÝ PRENOSOVÝ KANÁL:

$$P(\text{CHYBA v } 1) = P(\text{CHYBA v } 0)$$

V PRAXI MÔŽE DÔJSŤ K ZHLUKOVANIU CHÝB (UDRIE BLESK ATĎ.)
RIEŠENIE: BLOKY NEPRENÁŠAME ZA SEBOU, ALE PO ČASTIACH



SHANNON UKÁZAL, ŽE JE MOŽNÉ PRENÁŠAŤ DATA "SPOLAHLIVO" TAK, ŽE K PRENOSU k BITOV POUŽÍVAM n BITOV, POKIAĽ

$$k < (1 - H(p))\, n,$$

KDE p JE PRAVDEPODOBNOSŤ CHYBY.

"SPOLAHLIVOSŤ" $\equiv$ PRAVDEPODOBNOSŤ CHYBY JE NAJA' AK $n \to \infty$, POTOM PR. CHYBY $\to 0$ ... $2^{-\delta n}$

$m \rightsquigarrow m'$ ... KOĽKO CHÝB UVIDÍME?

KEĎ POSIELAM n BITOV ... $X_1, \dots, X_n \in Alt(p)$

N.V. X_i ... DOŠLO K CHYBE NA i-TOM MIESTE.

ZREJME OČ. POČET CHÝB JE $\mathbb{E} \sum X_i = np$.

<u>MARKOVOVA NEROVNOSŤ</u>: AK X JE NEZÁPORNÁ N.V.

$$\Rightarrow P(X \geq t) \leq \frac{\mathbb{E}X}{t}$$

<u>CHEBYSHEVOVA NEROVNOSŤ</u>: $\forall a > 0$

$$P(|X - \mathbb{E}X| > a) \leq \frac{\mathbb{V}ar\, X}{a^2}$$

DÔKAZ. $P(|X - \mathbb{E}X| > a) =$

$$P(\underbrace{(X - \mathbb{E}X)^2}_{\mathbb{V}ar\, X} > a^2) \leq \frac{\mathbb{V}ar\, X}{a^2}$$

15.10.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

CHERNOFFOVA NEROVNOSŤ: $X_1, \dots, X_n$ NEZÁVISLÉ 0/1 N.V., $X_i \sim Alt(p_i)$.

NECH $X = \sum_{i=1}^{n} X_i$, $\mu = \mathbb{E}X = \sum_{i=1}^{n} p_i$.

PRE $0 < \delta < 1$ PLATÍ:

$$P(X \geq (1+\delta)\mu) \leq \left[\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right]^{\mu}$$

$$P(X \leq (1-\delta)\mu) \leq e^{-\frac{1}{2}\mu\delta^2}$$

PRE $0 < \delta < 1$ TIEŽ:

$$P(X \geq (1+\delta)\mu) \leq e^{-\frac{1}{2}\mu\delta^2}.$$

PRÍKLAD: $P(X \geq \frac{3}{2}pn) \leq$

$$\leq e^{-\frac{1}{2}\cdot\frac{1}{4}\cdot pn} = \underline{\underline{e^{-\frac{pn}{8}}}}$$

CHCEME KÓD, KT. VIE OPRAVIŤ $\frac{3}{2}pn$ CHÝB,

TJ. $[n, \dots, \frac{3}{2}pn]$

PREDPOKLADÁME, ŽE $p < \frac{2}{3}$.

VO ŠEOBECNOSTI $[n, \dots, (1+\delta)pn]$

KDE $0 < \delta < 1$ SME ZAFIXOVALI.

$$k \approx (1 - H((1+\delta)p))n$$

ZNIŽOVANÍM δ SA MÔŽEM PRIBLÍŽIŤ K IDEÁLU.

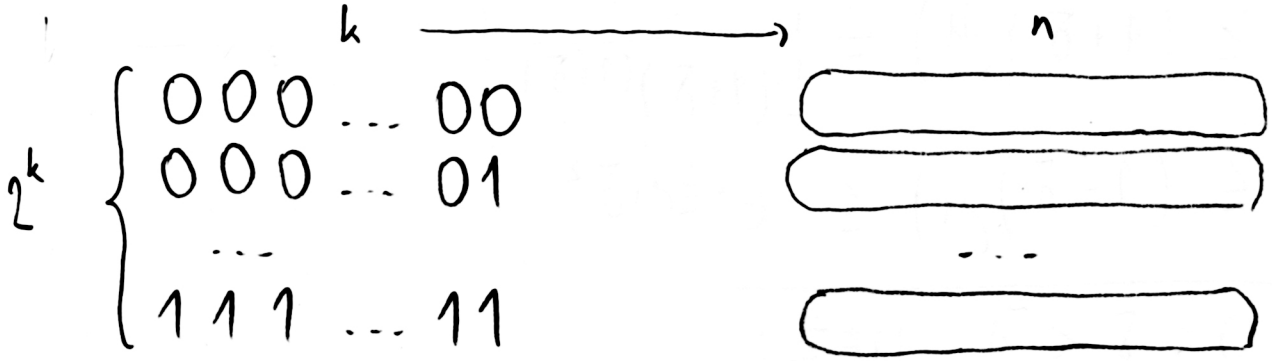
CIEĽ SHANNONA

$m \rightsquigarrow m'$ PRAVDEPODOBNOSŤ CHYBY p

$|m| = |m'| = n$

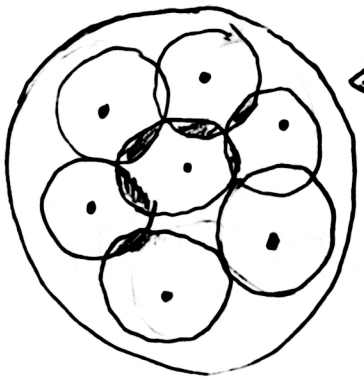
CHCEME OPRAVIŤ: $[(1+\delta)p]n$ CHÝB, $0<\delta<1$

$$k := (1 - H(p(1+\delta)) - \delta)n$$



ČO FUNGUJE VEĽMI DOBRE ... KÓD ZVOLÍME NÁHODNE!

... KÓD BUDE DOBRE ROZPRESTRENÝ V $\{0,1\}^n$



POVOLÍME EXPONENCIÁLNE MALÉ PREKRYVY

22.10.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

VETA (SHANNON): PRE $\forall\ 0 < p < \frac{1}{2}$

$\forall\ 0 < \delta, \varepsilon < 1\ \ \exists c > 0\ \ \forall n \geq c$

$k := (1 - H(p+\delta) - \varepsilon)n$

EXISTUJE KÓD $E : \{0,1\}^{k-1} \to \{0,1\}^n$ T.Ž.

PRE KAŽDÚ SPRÁVU JE PRAVDEPODOBNOSŤ CHYBNÉHO PRENOSU $\leq 2^{-\varepsilon n}$, AK PRAVDEPODOBNOSŤ CHYBY NA KAŽDOM BITE JE $\leq p$.

PREČO $p < \frac{1}{2}$? AK $p > \frac{1}{2}$, POTOM NEGUJ BITY $\Rightarrow$ DOSTANEME $1-p$. ($p \neq \frac{1}{2}$, PRETOŽE $H(\frac{1}{2}) = 1$)

NECH $X_i \overset{iid}{\sim} Alt(p)$, $\eta = (X_1, \dots, X_n)$

$P(|\eta| \geq (p+\delta)n) \leq e^{-\frac{1}{2}\delta^2 \cdot pn}$

PRAVDEPODOBNOSŤ, ŽE #CHÝB JE $\geq (p+\delta)n$ IDE K 0 S $n \to \infty$.

ĎALEJ BUDEME SKRÁTENE PÍSAŤ $\eta \in_p \{0,1\}^n$.

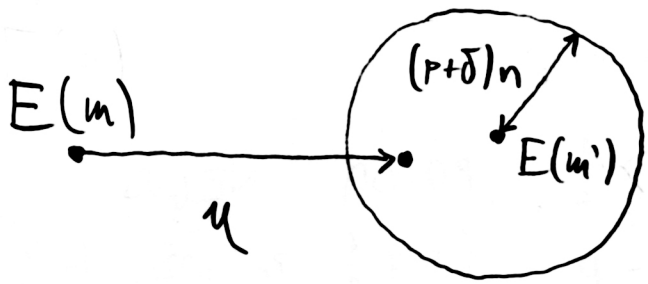
SPRÁVA $m \in \{0,1\}^k$ ... ZVOLME NEJAKÚ PEVNE.

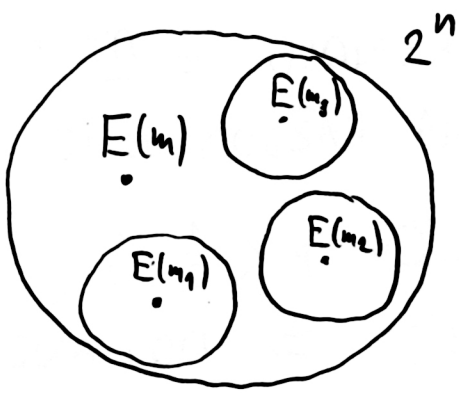
$$\Pr_{\substack{E \in_{1/2} \{0,1\}^{n \cdot 2^k} \\ \eta \in_p \{0,1\}^n}} \left[\begin{array}{l} \text{SPRÁVA } m \text{ PRI POUŽITÍ } E \\ \text{A CHYBY } \eta \text{ JE ZLE DEKÓD.} \end{array} \right] \leq$$

$$\leq \Pr_{E,\eta}\left(w(\eta) \geq (p+\delta)n\right) +$$

$$+ \Pr_{E,\eta}\left(\exists m' \neq m \mid E(m) + \eta \in \mathrm{Ball}_2\left(E(m'), (p+\delta)n\right)\right) \leq e^{-\Theta(n)}$$

- VYBERIEM η
- VYBERIEME E PRE $\forall$ SPRÁV OKREM m
- ZVOLÍME SI $E(m)$





$$E(m) + \eta \in \mathrm{Ball}_2\left(E(m'), (p+\delta)n\right) \Leftrightarrow$$

$$\Leftrightarrow \quad E(m) \in \mathrm{Ball}_2\left(E(m') + \eta, (p+\delta)n\right)$$

$$\Pr[\text{ZLÉ DEKÓDOVANIE}] \leq \frac{2^k \cdot 2^{H(p+\delta)n}}{2^n} = 2^{-\varepsilon n}$$

$$= \frac{\#\text{GÚĽ} \cdot \text{VELKOSŤ}}{\text{CELÝ PRIESTOR}}$$

$e^{-\Theta(n)}$ $\longrightarrow$ PRAVDEPODOBNOSŤ CHYBY

22.10.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

CHCEME KÓDOVANIE, KT. BUDE FUNGOVAŤ PRE <u>VŠETKY SPRÁVY</u>:

	E_1	E_2	...	$E_{2^n \cdot 2^k}$
0 .. 00				
0 .. 01				
1 .. 11				

PRAVDEPODOBNOSŤ CHYBNÉHO DEKÓDOVANIA PRI NÁHODNOM η.

SÚČET V KAŽDOM RIADKU: (ODHADNUTÁ PRAVD. JE PRIEMER)

$$\sum_{E_i} P_{\eta}\left[\text{ZLÉ PRI } E_i\right] \leq 2^{n2^k} \cdot 2^{-\Theta(n)}$$

$$\sum_{\text{TABUĽKA}} \leq 2^k \cdot 2^{n2^k} \cdot 2^{-\Theta(n)}$$

$\Rightarrow$ EXISTUJE STĹPEC SO SÚČTOM $2^k \cdot 2^{-\Theta(n)}$

$\Rightarrow$ TEN SI VYBERIEME ... E^*

ZATIAĽ MÁME LEN PRIEMER (ČO KEĎ NIEKDE V BUNKE JE VEĽA?)

NAJVIAC POLOVICA SPRÁV MÁ V TABUĽKE V POLOŽKE E^* HODNOTU VÄČŠIU NEŽ $2 \cdot 2^{-\Theta(n)}$

$\Rightarrow$ STAČÍ POUŽIŤ TÝCH 2^{k-1} ZVYŠNÝCH RIADKOV A SME HOTOVÍ ...

NÁHODNÉ KÓDY SÚ OK, ALE PROBLÉM:

- TREBA DOSŤ VEĽKÚ TABUĽKU
- PROBLEMATICKÉ DEKÓDOVANIE

REED - SOLOMONOVE KÓDY

- KONEČNÉ TELESÁ (KOMUTATÍVNE)
- LINEÁRNE KÓDY

FAKT: POLYNÓM STUPŇA ℓ NAD TELESOM $GF[m]$ $(\ell < m)$ MÁ NAJVIAC ℓ KOREŇOV.
(PLATÍ AJ V $\mathbb{R}$, V $\mathbb{C}$ PRÁVE ℓ KOREŇOV)

C JE LINEÁRNY KÓD NAD $GF[q]$, $(q = p^k)$
... VEKTOROVÝ PRIESTOR NAD $GF[q]$:

$\forall x, y \in C : x + y \in C$
$\forall x \in C \ \forall a \in GF[q] : ax \in C.$

VLASTNOSTI LINEÁRNYCH KÓDOV:

- DAJÚ SA POPÍSAŤ GENERUJÚCOU MATICOU
  $x \in GF[q]^k \Rightarrow y = x \cdot G \in GF[q]^n.$

22.10.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

$x, y \in GF[q]^n$

$\Delta(x,y) = wt(x-y)$ ... HAMMINGOVA VÁHA

(POČET $\neq 0$ PRVKOV)

- ZAUJÍMA NÁS MINIMÁLNA VZDIALENOSŤ KÓDU

<u>VETA</u>: POKIAĽ C JE LINEÁRNY KÓD, POTOM

$$\Delta(C) = \min_{x \in C, x \neq 0} wt(x)$$

<u>DÔKAZ.</u> $\Delta(x,y) = wt(x-y)$ A $x-y \in C$.

REED-SOLOMONOVE KÓDY

$n, k, GF[q], \underline{\underline{q \geq n}}$ (q MOCNINA PRVOČÍSLA)

$[n, k, n-k+1]_q$

$\alpha_1, \dots, \alpha_n \in GF[q]$ ... PEVNE ZVOLENÉ, RÔZNE

$m \in GF[q]^k$ ... SPRÁVA, $m = (m_0, \dots, m_{k-1})$

POLYNÓM: $p_m(x) = m_0 + m_1 x + \dots + m_{k-1} x^{k-1}$

KÓD: $(p_m(\alpha_0), p_m(\alpha_1), \dots, p_m(\alpha_n))$

REED-SOLOMONOV KÓD JE LINEÁRNY:

$m_1, m_2 \in GF[q]^k \Rightarrow p_{m_1+m_2}(x) \equiv p_{m_1}(x) + p_{m_2}(x)$

MINIMÁLNA VZDIALENOSŤ JE DANÁ NAJMENŠOU HAMMINGOVOU VÁHO SLOVA Z C, $\neq 0$.

POLYNÓM STUPŇA $k-1$ MÁ NAJVIAC $k-1$ KOREŇOV

$\Rightarrow$ NAJVIAC $k-1$ NÚL ...

MINIMÁLNA VZDIALENOSŤ $\geq n-k+1$.

PRE $k=\varepsilon n$ JE RS-KÓD $[n, \varepsilon n, n-\varepsilon n+1]_q$

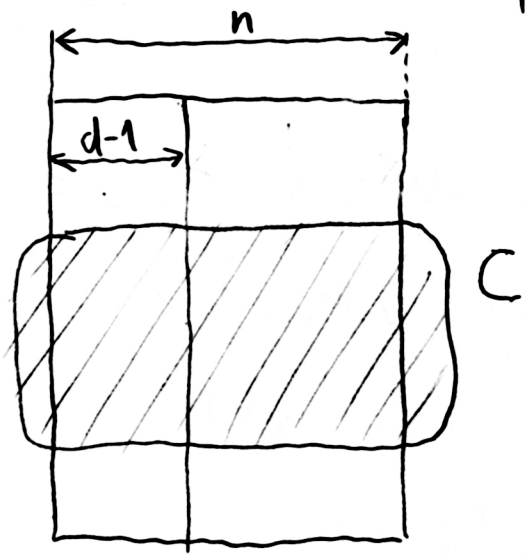
PROBLÉM: VEĽKOSŤ ABECEDY JE PRÍLIŠ VEĽKÁ

SINGLETONOVA MIERA

RS-KÓD SA NEDÁ ZLEPŠIŤ.

$[n, k, d]_q$ KÓD $\Rightarrow n \geq k+d-1$.

DÔKAZ. $|C| = q^k$, CELÝ PRIESTOR ... q^n



ZMAŽ $d-1$ ZNAKOV

... STÁLE MÁM KÓD

D. $q^k \leq q^{n-(d-1)}$

$\Rightarrow k \leq n-d+1$. $\square$

29.10.2010 FF
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

SHANNON

$k \approx (1 - H(p))n$

"OPRAVUJE pn CHÝB" $\Rightarrow$ $\Delta = 2pn + 1$

NIE JE ZNÁMY ŽIADEN KÓD, KT. BY TOTO VEDEL

REED-SOLOMONOVE KÓDY

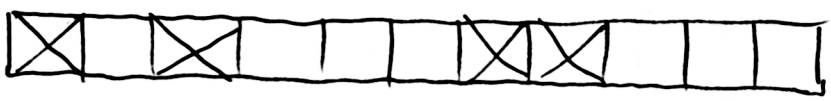
$m \in GF[q]^k \longmapsto (p_m(\alpha_1), \dots, p_m(\alpha_n))$

NECH $q = 2^a$

$k \cdot a$ BITOV $\rightarrow$ $n\,a$ BITOV
$a \geq \log_2 n$ (PRETOŽE $q \geq n$)
} POŽIADAVKY

SKÚSME $a = \log_2 n$, TJ.

$k \cdot \log_2 n \longmapsto n \cdot \log_2 n$



n ... PRVOK Z $GF[q]$

$\lfloor d/2 \rfloor$ CHÝB, d - VZDIALENOSŤ

$n \log n$ ... Z $GF[2]$

PRE $k = \frac{n}{2}$, $[n, \frac{n}{2}, \frac{n}{2}]_q$

$\rightsquigarrow [n \log n, \frac{n}{2} \log n, \frac{n}{2}]_2$

$\Rightarrow$ - RELATÍVNA VZDIALENOSŤ SA ZHORŠÍ

- RATE JE OK. $k/n \to 1/2$.

NECH $N = n \cdot \log n$, $k = n-4$, TJ $K = N - 4\log n$

$\Rightarrow$ $[N, (n-4)\log n, 5]_2$ KÓD

- OPRAVÍ 2 CHYBY

- $$Vol_2(n,2) = \binom{n}{2} + \binom{n}{1} + 1 \approx \frac{n^2}{2}$$

$$\# \text{SLOV} \approx \frac{2^N}{2^{-1}N^2} \approx 2^{N - 2\log N + o(1)}$$

ČO NIE JE ZLÉ: $2\log N$ VS. $4\log N$

- PROBLÉM: NEMÁ KONŠTANTNÚ REL. VZDIALENOSŤ
- ALE JE TO ZAUJÍMAVÉ...

<u>GENERUJÚCA MATICA RS-KÓDU:</u>

$$G = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{bmatrix}$$

29.10.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

ZOVŠEOBECNENIE NA REED-MÜLLEROVE KÓDY

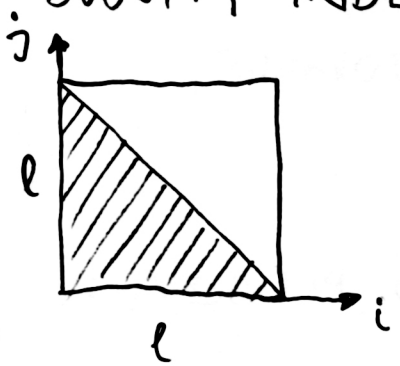
- VIAC PREMENNÝCH ⇒ MENŠIE TELESO

POLYNÓMY V 2 PREMENNÝCH :

ℓ .. CELKOVÝ STUPEŇ

$$\sum_{\substack{i+j \le \ell \\ 0 \le i,j}} m_{i,j} x^i y^j = p_m(x,y)$$

DVOJITÝ INDEX, SPRÁVU PÍŠEME DO MATICE :



$\frac{\ell^2}{2}$ PRVKOV

BERIEME IBA PRVKY, KDE $i+j \le \ell$

$(\alpha_1, \beta_1), \dots, (\alpha_n, \beta_n) \in GF[q]^2$

⇒ KÓD $(p_m(\alpha_1, \beta_1), \dots, p_m(\alpha_n, \beta_n))$

TYPICKY $n = q^2$ A VOLÍME VŠETKY DVOJICE $(\alpha, \beta) \in GF[q]^2$.

OPÄŤ SA JEDNÁ O LINEÁRNY KÓD.

MINIMÁLNA VZDIALENOSŤ

- NAJMENŠIA VÁHA NENULOVÉHO PRVKU
- KOĽKO JE KOREŇOV PRI TOM POLYNÓME

LEMMA (SCHWARZ-ZIPPEL): $\forall m, l \in \mathbb{N}$ KONEČNÉ TELESO $\mathbb{F}$, $S \subseteq \mathbb{F}$, POLYNÓM $p \neq 0$ m PREMENNÝCH CELKOVÉHO STUPŇA $\leq l$. POTOM p MÁ NAJVIAC $l \cdot |S|^{m-1}$ KOREŇOV V MNOŽINE $S^m \subseteq \mathbb{F}^m$.

$$P\left(p(x) = 0,\ x \in S^m\right) \leq \frac{l}{|S|}$$

POZNÁMKA: DÁ SA POUŽIŤ NA TESTOVANIE, ČI $p(\dots) \equiv 0$.

U VIACERÝCH PREMENNÝCH JE TROCHU PROBLÉM:

PRE 1 PREMENNÚ:

- $p = \sum \prod (x + ..)$ ... VYHODNOŤ A JE TO
- ROZNÁSOB $\rightarrow$ MAXIMÁLNY STUPEŇ $\leq$ DĹŽKA ZÁPISU A BUDE TO POLYNOMIÁLNE ...

PRE VIAC PREMENNÝCH:

$(x+y)^n$ ... NEMUSÍ SA DAŤ VYHODNOTIŤ A ZAPÍSAŤ CEZ FORMULU TVARU: $\sum m_{ij} x^i y^j$ V POL. VEĽKOSTI.

29.10.2010 Fr
PETER ČERNO

NTINO85 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

<u>DÔKAZ</u>. INDUKCIA PODĽA # PREMENNÝCH m.

$m=1$: ZÁKLADNÁ VETA ALGEBRY.

$m+1$: NECH x_{m+1} SA VYSKYTUJE V s-TEJ MOCNINE

$$P(x_1, \dots, x_{m+1}) = p_s(x_1, \dots, x_m)\, x_{m+1}^s + p_{s-1}(x_1, \dots, x_m)\, x_{m+1}^{s-1} + \dots + p_0(x_1, \dots, x_m).$$

KEDY TO MÔŽE BYŤ 0?

$x_1, \dots, x_m \in S^m$:

a) AK $p_s(x_1, \dots, x_m) = 0$, x_{m+1} ZVOLÍME ĽUBOVOĽNE

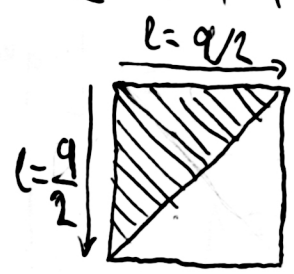
... NAJVIAC $(l-s)|S|^{m-1} \cdot |S|$ MOŽNOSTÍ

b) AK $p_s(x_1, \dots, x_m) \neq 0$, x_{m+1} ZVOLÍME TAK, ABY VÝSLEDOK BOL 0

... PRE x_{m+1} JE NAJVIAC s MOŽNOSTÍ

<u>SPOLU</u>: $(l-s)|S|^{m-1} \cdot |S| + s \cdot |S|^m \leq l \cdot |S|^m$. $\square$

UVAŽUJME $q \approx \sqrt{n}$ ...



$n = q^2$, $l = \frac{q}{2}$, $k = \frac{l^2}{2} = \frac{q^2}{8}$

$$\Rightarrow \left[q^2, \frac{q^2}{8}, q^2 - \frac{q^2}{2}\right]_q = \left[q^2, \frac{q^2}{8}, \frac{q^2}{2}\right]_q$$

$n = q^2 \Rightarrow$ BERIEME $\forall$ DVOJICE TELESA.

$|S| = q$, # KOREŇOV $\leq \ell \cdot |S| = \frac{q^2}{2}$

REED-MÜLLEROVE KÓDY PRE m PREMENNÝCH

PREMENNÝCH ... m
CELKOVÝ STUPEŇ ... ℓ

$$\sum_{\substack{i_1 + \dots + i_m \leq \ell \\ 0 \leq i_1, \dots, i_m}} w_{i_1, \dots, i_m} x_1^{i_1} \dots x_n^{i_m} = P_m$$

$$(P_m(\alpha_1, \dots, \omega_1), \dots, P_m(\alpha_n, \dots, \omega_n))$$

$$(\alpha_1, \dots, \omega_1), \dots, (\alpha_n, \dots, \omega_n) \in GF[q]^m$$

$k = \binom{m+\ell}{\ell} \approx c \cdot m^\ell$ ... DĹŽKA SPRÁV

$n = q^m$ ... DĹŽKA KÓDOVÉHO SLOVA

PRE $\ell = \frac{q}{2}$: $[q^m, \Theta(m^\ell), q^m - \frac{q}{2} q^{m-1}]_q =$

$= [q^m, \Theta(\sqrt{m^q}), \frac{q^m}{2}]_q$

$q=2, \ell=1$ ... $[2^m, \Theta(m), 2^{m-1}]_2$ <u>HADAMARDOV KÓD</u>

$w_1, \dots, w_m \in \{0,1\}$, $P_w(x_1, \dots, x_k) = \sum_i w_i x_i$

$$w \longmapsto (P_w(0, \dots, 0), P_w(0, \dots, 1), \dots, P_w(1, \dots, 1)).$$

05.11.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

MEZE PRO KÓDY

CHCEME KÓDY, KDE

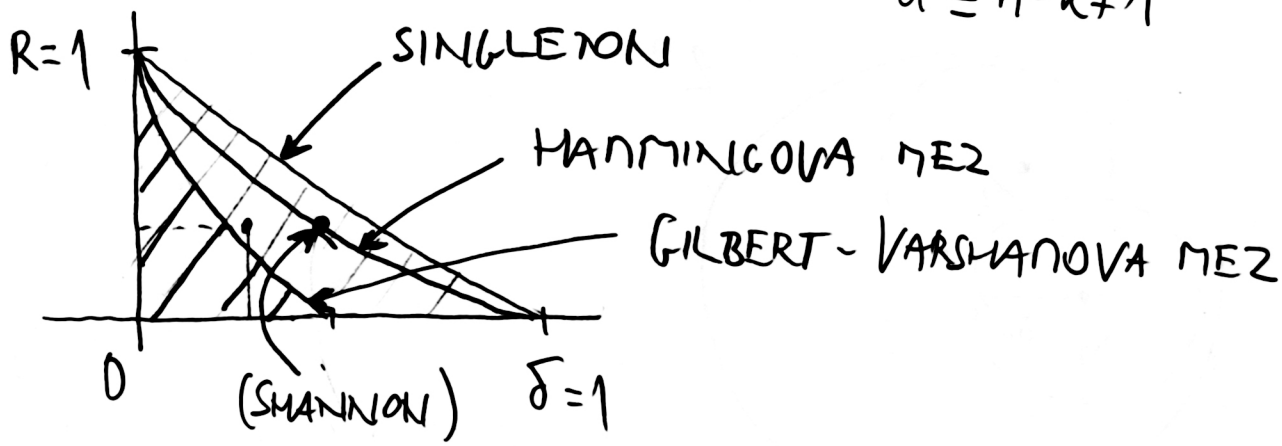
R ... RATE JE KONŠT.

δ ... REL. MIN. VZDÁLENOST JE KONŠT.

n ... DÉLKA KÓDU

- SINGLETON : $\delta + R < 1$ $\quad (n, k, d)$

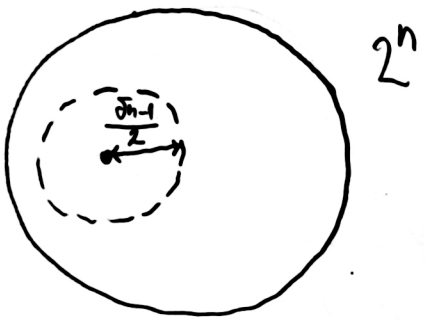
  $d \leq n - k + 1$



- OBJEMOVÁ MEZ (HAMMINGOVA) :

  (BIN. KÓDY)

$$|C| \leq \frac{2^n}{Vol_2\left(n, \frac{\delta n - 1}{2}\right)}$$



$$R \leq 1 - H\left(\frac{\delta}{2}\right) + o(1)$$

SHANNON: $R < 1 - H(p) \approx 1 - H(\frac{\delta}{2})$

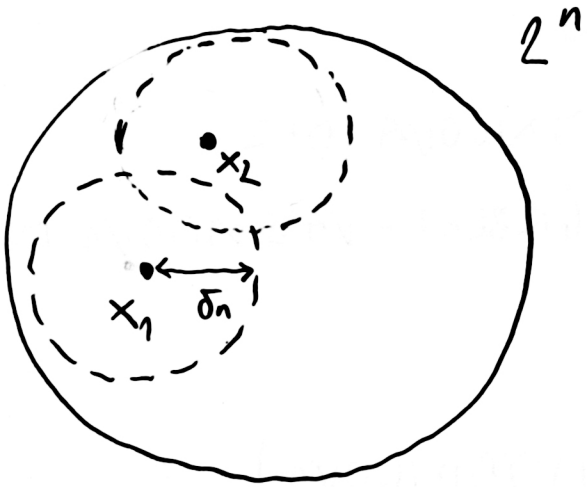
GILBERT-VARSHAMOVA MEZ

$\exists C: \quad R \geq 1 - H(\delta)$

GILBERT: CHCEME KÓD S PARAMETRAMI:

$(n, k, \delta n)$

HLADOVÝ ALGORITMUS:



$S := \{0,1\}^n$ ... POVOLENÉ SLOVÁ

i-TÝ KROK:

VÝBER $x_i \in S$

$S := S \setminus Ball_2(x_i, \delta n)$

OPAKUJ DOKEDY $S \neq \emptyset$

DOSTANEME $C = \{x_1, \dots, x_K\}$.

KEDY SA KONŠTRUKCIA ZASTAVÍ?

05.11.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

$|S| = 2^n$ NA ZAČIATKU

$$|S| \to |S| - \underbrace{Vol_2(n, \delta n)}_{2^{H(\delta)n}}$$

$$\Rightarrow K \geq \frac{2^n}{2^{H(\delta)n}} = 2^{(1-H(\delta))n}$$

$$K = 2^k \Rightarrow k \geq (1-H(\delta))n. \quad \blacksquare$$

LINEÁRNY KÓD (VARSHAMOV)

EXISTUJÚ 2 KONŠTRUKCIE

KONTROLNÁ MATICA KÓDU (n, k, d)

$H \in GF[2]^{n \times (n-k)}$ $\quad C = \{ y \in \{0,1\}^n \mid yH = 0 \}$.

$$H = \begin{bmatrix} \cdots\cdots \\ \cdots\cdots \\ \\ \cdots\cdots \end{bmatrix} \begin{matrix} \\ \\ \vdots \\ \\ \end{matrix}$$

ĽUBOVOLNÁ
$(d-1)$-TICA RIADKOV $\quad (*)$
... LINEÁRNE NEZÁVISLÁ

ZOSTROJÍME MATICU H S TOUTO VLASTNOSŤOU.
(ITERATÍVNE)

PREDPOKLADAJME, ŽE UŽ MÁME ℓ RIADKOV.
HĽADÁME ĎALŠÍ RIADOK $x \in \{0,1\}^{n-k}$.
PODMIENKA (*) SA PORUŠÍ IBA VTEDY, KEĎ x JE LIN. KOMBINÁCIA NEJAKÝCH $d-2$ RIADKOV. TJ. CHCEME:

$\forall \leq d-2$ RIADKOV : x NIE JE ICH SÚČTOM.

$\binom{\ell}{0} + \binom{\ell}{1} + \binom{\ell}{2} + \dots + \binom{\ell}{d-2}$ = HORNÝ ODHAD NA POČET ZAKÁZANÝCH $x \in \{0,1\}^{n-k}$.

PRE $\ell = n$: $\sum_{i=0}^{d-2} \binom{n}{i} = Vol_2(n, d-2) \leq 2^{H(\delta)n}$.

POČET MOŽNOSTÍ PRE x JE 2^{n-k}. $d = \delta n$.

$2^{H(\delta)n} \leq 2^{n-k}$

TJ. $k \leq (1 - H(\delta))n$.

$\rightarrow$ H O ROZMEROCH $n \times (n-k)$

$C = \{ y \in \{0,1\}^n \mid yH = 0 \}$

$\dim C \geq n - (n-k) = k$.

DOSTÁVAME $R \geq 1 - H(\delta)$.

05.11.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

PRAVDEPODOBNOSTNÁ KONŠTRUKCIA:

NÁHODNE ZVOLÍME GENERÚCU MATICU:

$G \in GF[2]^{k \times n}$.

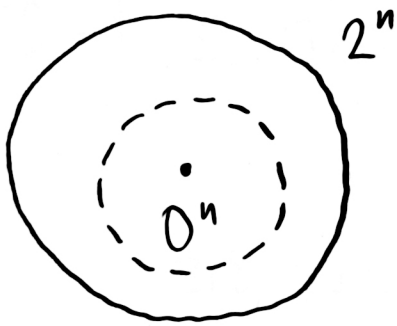
$2^k - 1$ možností

POTREBUJEME: $\forall x \in \{0,1\}^k \setminus \{0^k\}$:

$$x G \notin Ball_2(0^n, d-1).$$

ZAFIXUJME x. AKÁ JE PRAVDEP., ŽE

$$x G \in Ball_2(0^n, d-1) \quad ?$$



$x G$ JE UNIFORMNE ROZDELENÝ NÁHODNÝ VEKTOR.

$$\Rightarrow \Pr_G[x G \in Ball_2(0^n, d-1)] = \frac{Vol_2(n, d-1)}{2^n}$$

$$\Pr_G[x_0 G \in Ball_2(\dots) \vee \dots \vee x_{2^k-2} G \in \dots] \leq$$

$$\leq \sum_{i=0}^{2^k-2} \Pr_G[\dots] \leq 2^k \cdot \frac{2^{H(\delta)n}}{2^n}.$$

KEĎ $2^k < 2^{(1-H(\delta))n}/2$

$\Rightarrow \Pr[\ldots] \leq \frac{1}{2}$

PRE $k \leq (1-H(\delta))n - 1$,

POTOM G VYBRANÁ NÁHODNE

JE $[n, k, \delta n]_2$ KÓD S PRAVDEP. $\geq \frac{1}{2}$.

... TO JE NP-ŤAŽKÉ OTESTOVAŤ.

MOŽNÉ RIEŠENIE ... VOLÍME NAPR.

$$k \leq (1-H(\delta))n - 100$$

$\longrightarrow$ PRAVDEPODOBNOSŤ KOREKTNOSTI $\geq 1 - 2^{-100}$ ...

NP-ÚPLNÝ PROBLÉM:

PRE $y \in \{0,1\}^n$ NÁJSŤ NAJBLIŽŠIE SLOVO Z KÓDU ...

WOZENCRAFTOV SÚBOR KÓDOV

REED-SOLOMONOV. K. $\rightarrow$ BINÁRNE KÓDY

$C_1, C_2, C_3, \ldots, C_t$ ... SÚBOR KÓDOV Z 2^n:

1) C_i SÚ LINEÁRNE
2) $\bigcup_{i=1}^{t} C_i = 2^n$
3) $i \neq j \Rightarrow C_i \cap C_j = \{0^n\}$
4) $\forall i : |C_i| = 2^k$

... WOZENCRAFTOV SÚBOR

05.11.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

$$t = \frac{2^n - 1}{2^k - 1} \quad \ldots \quad t \text{ JE CELÉ} \iff k \mid n$$

<u>VETA</u>: $C_1, \ldots, C_t$ WOZENCRAFTOV SÚBOR, $\forall\, 0 < \varepsilon < 1$, $\forall d$ T.Ž. $\varepsilon t \geq Vol_2(n, d-1)$, POTOM ASPOŇ $(1-\varepsilon)$-TINA Z KÓDOV $C_1, \ldots, C_t$ MÁ MINIMÁLNU VZDIALENOSŤ ASPOŇ d.

<u>DÔKAZ</u>: (TRIVIÁLNY)

KAŽDÉ C_i S MIN. VZDIALENOSŤOU $< d$ MUSÍ OBSAHOVAŤ SLOVO $\neq 0^n$ Z $Ball_2(n, d-1)$. KEĎŽE $Vol_2(n, d-1) \leq \varepsilon t$, NEMÔŽE ICH BYŤ (VZHĽADOM K DISJ.) VIAC AKO εt. $\square$

NAPR. PRE $2 \mid n$, $k = \frac{n}{2}$; $\varepsilon = \frac{1}{2}$

$$t = \frac{2^n - 1}{2^k - 1} = 2^k + 1$$

KDE $2^{k-1} \geq Vol_2(n, d-1)$

PRE $d = \delta n$, $k > H(\delta) n$.

PROBLÉM: AKO SKONŠTRUOVAŤ $C_1, \ldots, C_t$?

VEZMIME SI $\alpha_1, \alpha_2, \dots, \alpha_\ell \in GF[2^k]$

AK $\alpha_1, \dots, \alpha_i = 0$, POTOM $\alpha_{i+1} = 1$.

TJ. $(0, 0, 0, 1, \alpha_{i+2}, \alpha_{i+3}, \dots, \alpha_\ell)$

KDE $\ell = \frac{n}{k}$.

$C_{\alpha_1, \dots, \alpha_\ell} = \{ (x\alpha_1, x\alpha_2, \dots, x\alpha_\ell) \mid$

$x \in GF[2^k] \}$. (S PRIRODZENOU

REPREZENTÁCIOU $GF[2^k] = \{0,1\}^k$)

$GF[2^k]$ = POLYNÓMY STUPŇA $\leq k-1$ NAD $GF(2)$

S POČÍTANÍM mod r, KDE r JE

IREDUCIBILNÝ POLYNÓM STUPŇA k.

PRIR. REPREZENTÁCIA .... k KOEF. Z $GF[2]$.

UVAŽUJME $(\alpha_1, \dots, \alpha_\ell) \neq (\alpha_1', \dots, \alpha_\ell')$.

CHCEME OVERIŤ, ŽE:

$$\underbrace{C_{\alpha_1, \dots, \alpha_\ell} \cap C_{\alpha_1', \dots, \alpha_\ell'}}_{(0, 0, \dots, x, x\alpha_{i+1}, \dots, x\alpha_\ell) \quad \dots \quad \cdot x^{-1}} = \{0^n\}.$$

$\rightarrow (0, 0, \dots, 1, \alpha_{i+1}, \dots, \alpha_\ell) =$

$= (0, 0, \dots, 1, \alpha_{i+1}', \dots, \alpha_\ell')$ ↯

OSTATNÉ PODMIENKY SÚ ZREJME ... □

12.11.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

WOZENCRAFTOV SÚBOR

$n, k, t = \frac{2^n - 1}{2^k - 1}, \quad k | n$

SÚBOR KÓDOV $C_1, \dots, C_t \subseteq \{0,1\}^n$
LINEÁRNE, $|C_i| = 2^k$
$\bigcup C_i = \{0,1\}^n, \quad i \neq j \Rightarrow C_i \cap C_j = \{0^n\}$.

VETA: $0 < \varepsilon < 1, \quad 0 < \delta < 1$

$\varepsilon t \geq Vol_2(n, \delta n) \Rightarrow$ ASPOŇ $(1-\varepsilon)t$ KÓDOV MÁ MIN. VZDIALENOSŤ $\geq \delta n$.

KONSTRUKCIA: $\alpha_1, \dots, \alpha_t \in GF[2^k]$

$(0, 0, \dots, 0, 1, \alpha_{i+1}, \dots, \alpha_t)$

$C_{\alpha_1, \dots, \alpha_t} = \{ (x\alpha_1, \dots, x\alpha_t) \mid x \in GF[2^k] \}$

x ... k-TICA BITOV ... OZNAČUJEME AKO $\hat{x} \in \{0,1\}^k$

... $P_x(y) = x_0 + x_1 y^1 + x_2 y^2 + \dots + x_{k-1} y^{k-1}$

PODOBNE $P_\alpha(y) = \alpha_0 + \alpha_1 y^1 + \alpha_2 y^2 + \dots + \alpha_{k-1} y^{k-1}$

EXISTUJE 0-1 MATICA $k \times k$ G_α:

$\hat{x} G_\alpha = \widehat{x \cdot \alpha}, \quad x, \alpha \in GF[2^k] \quad \hat{\cdot}$ ... REPR. $\{0,1\}^k$

GENERUJÚCA MATICA KÓDU $C_{\alpha_1, \dots, \alpha_t}$ JE:

$(G_{\alpha_1}, \dots, G_{\alpha_t})$.

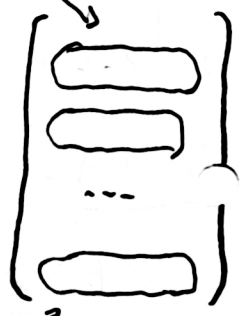
$$P_x(Y)\,P_\alpha(Y) = x_0 Y^0 \left(P_\alpha(y)\right) + x_1 Y^1 \left(P_\alpha(Y)\right) + \dots$$
$$\dots + x_{k-1} Y^{k-1} \left(P_\alpha(y)\right) \qquad (\mathrm{mod}\ r(y))$$

KDE $r(y)$ JE IREDUCIBILNÝ POLYNÓM PRE DANÉ TELESO

ČLENY: $Y^0 \cdot \left(P_\alpha(y)\right) \mod r(y)$

$\dots$

$Y^{k-1} \cdot \left(P_\alpha(y)\right) \mod r(y)$

$=$ 

SI MÔŽEM PREDPOČÍTAŤ ...

TO JE VLASTNE MATICA G_α ■

- OPERÁCIA PRIDANIA PARITY:

$$(n, k, 2t-1)_2 \longrightarrow (n+1, k, 2t)_2$$

$$w = (w_0, \dots, w_{n-1}) \rightarrow (w_0, \dots, w_{n-1}, w_n),$$

KDE $w_n = \sum_{i=0}^{n-1} w_i \mod 2$.

PRE $x \neq y$, $\Delta(x,y) = 2t-1$

SA x A y LÍŠIA NA NEPÁRNOM POČTE MIEST $\Rightarrow$ MAJÚ RÔZNE PARITY

$\Rightarrow \Delta(x', y') = 2t$.

12.11.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI I

- OPERÁCIA VYPUSTENIA SÚRADNICE:

$$(n, k, d)_q \longrightarrow (n-1, k, d-1)_q$$

- OPERÁCIA RESTRIKCIE A VYPUSTENIA:

$$(n, k, d)_q \longrightarrow (n-1, k-1, d)_q$$

- RESTRIKCIA ABECEDY: $\Sigma \to \Sigma' \subseteq \Sigma$

$$C \to C \cap (\Sigma')^n$$

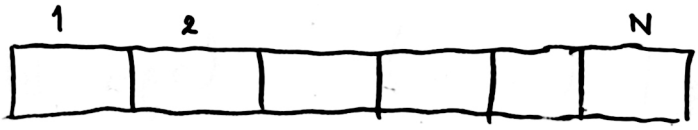
$$(n, k, d)_{|\Sigma|} \longrightarrow (n, ?, d)_{|\Sigma'|}$$

- OPERÁCIA SKLADANIA KÓDOV: $C_1 \cdot C_2$

$$Q = |\Sigma|, \quad q = |\Sigma'|$$

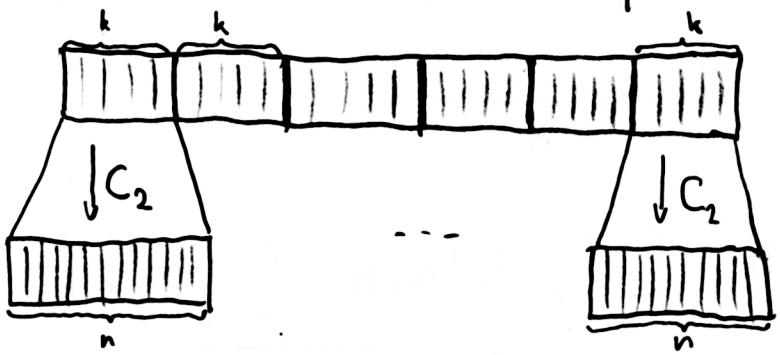
$$C_1 = (N, K, D)_Q \longrightarrow C_2 = (n, k, d)_q, \quad Q = q^k$$

C_1:



$$|C_1| = Q^K = q^{K \cdot k}$$

KAŽDÝ SYMBOL PRELOŽÍM DO q^k



A ZAKÓDUJEM

DOSTÁVAM KÓD $(N \cdot n, K \cdot k, D \cdot d)_q$.

RS - HADAMARDOV KÓD

$\mathbb{F} = \{\alpha_0, \dots, \alpha_{n-1}\}$

$n = |\mathbb{F}|$, $(n, k, n-k+1)_n$:

$$\underbrace{x_0, \dots, x_{k-1}}_{k} \mapsto P_x(Y) \mapsto (\underbrace{P_x(\alpha_0), \dots, P_x(\alpha_n)}_{n})$$

PREDPOKLADAJME, ŽE $n = 2^l$.

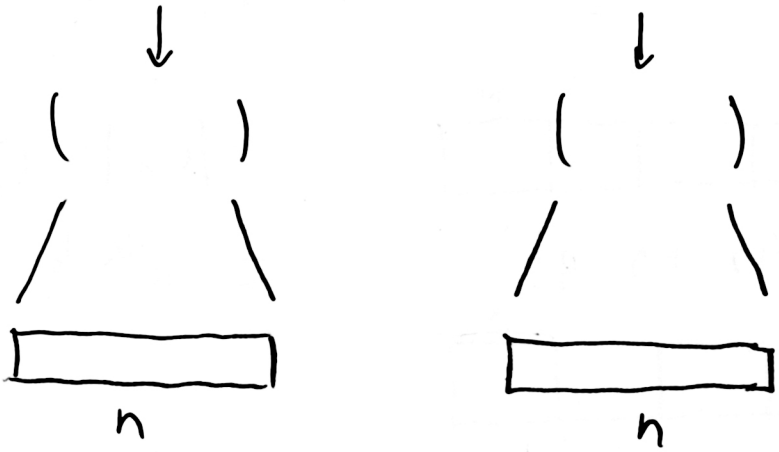
TJ. Z $(n, k, n-k+1)_n$ DOSTÁVAME:

$(n \log n, k \log n, n-k+1)_2$

TERAZ POUŽIJEME HARAMANDOV KÓD:

$(n, \log n, \frac{1}{2}n)_2$.

$(P_x(\alpha_0), \dots, P_x(\alpha_n))$



$\log n$ BITOV

$\downarrow$ HARAMANDOV KÓD

DOSTÁVAME KÓD: $(n^2, k \log n, \frac{n}{2}(n-k+1))_2$

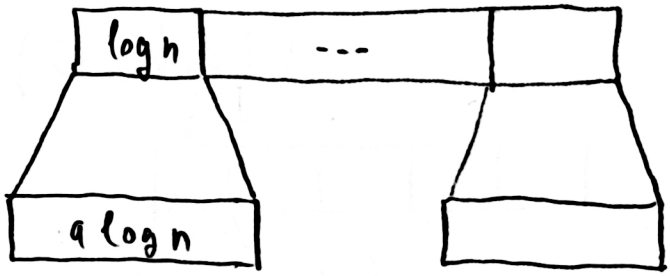
12.11.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽ. I

$\exists$ KÓD $C = (a\ell, \ell, \delta\ell)_2$

ZLOŽENÍM S REED-SOL. KÓDOM:

RS



$$(an \cdot \log n,\ \underline{\underline{k \cdot \log n}},\ \delta \log n\,(n-k+1))_2$$

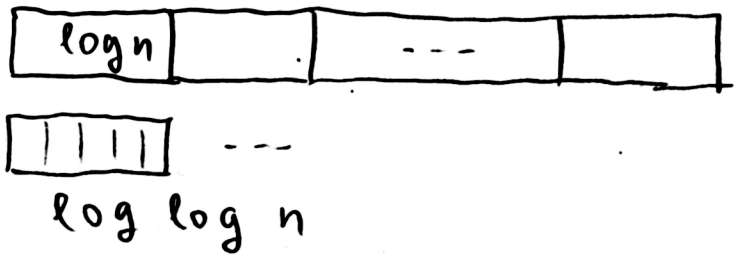
PREČO BY SME TO ROBILI, KEĎ VIEME NÁJSŤ C?

... KVÔLI EFEKTIVITE DEKÓDOVANIA.

PRE $\ell = O(\log n)$ NÁJDEME C V ČASE $2^{O(\ell)} = n^{O(1)}$.

TAKMEŽ KÓDOVANIE BEŽÍ V POL. ČASE.

ĎALŠIE ZLEPŠENIE: 2x ZLOŽÍM RS



$\Rightarrow$ KÓDOVANIE V ČASE $n \log^{O(1)} n$.

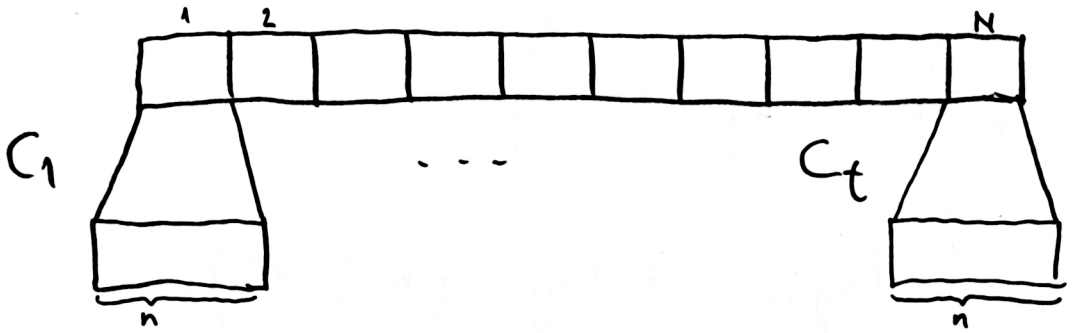
DEKÓDOVANIE :

NAPR. HRUBOU SILOU V POL. ČASE.

POUŽITIE WOZENCRAFTOVÉHO SÚBORU PRI SKLADANÍ

JUSTENSEN

$(N, K, D)_Q$



$Q = 2^k$

$$t = N = \frac{2^n - 1}{2^k - 1}$$

NAVIAC POŽADUJEME $n = 2k$
A $\varepsilon = 1/4$

DOSTÁVAME KÓD :

ODPOČÍTAM ŠPATNÉ C_i

$$(N \cdot n,\ K \cdot k,\ (D - \varepsilon \cdot N) \cdot \delta n)_2$$

δ ZVOLÍME TAK, ABY :

$$\varepsilon 2^k \geq Vol(2k, \delta 2k) \ \ldots$$

TJ. NAPR.

$$\delta \approx H^{-1}\left(\tfrac{1}{2}\right)$$

PRE RS ZVOLÍM $D = \frac{N}{2}$, TJ. DOSTÁVAM :

$$(N \cdot n,\ \underset{\frac{N}{2}}{K} \cdot \underset{\frac{n}{2}}{k},\ \tfrac{1}{4} N \delta n)_2$$

12.11.2010 FT
PETER ČERNO

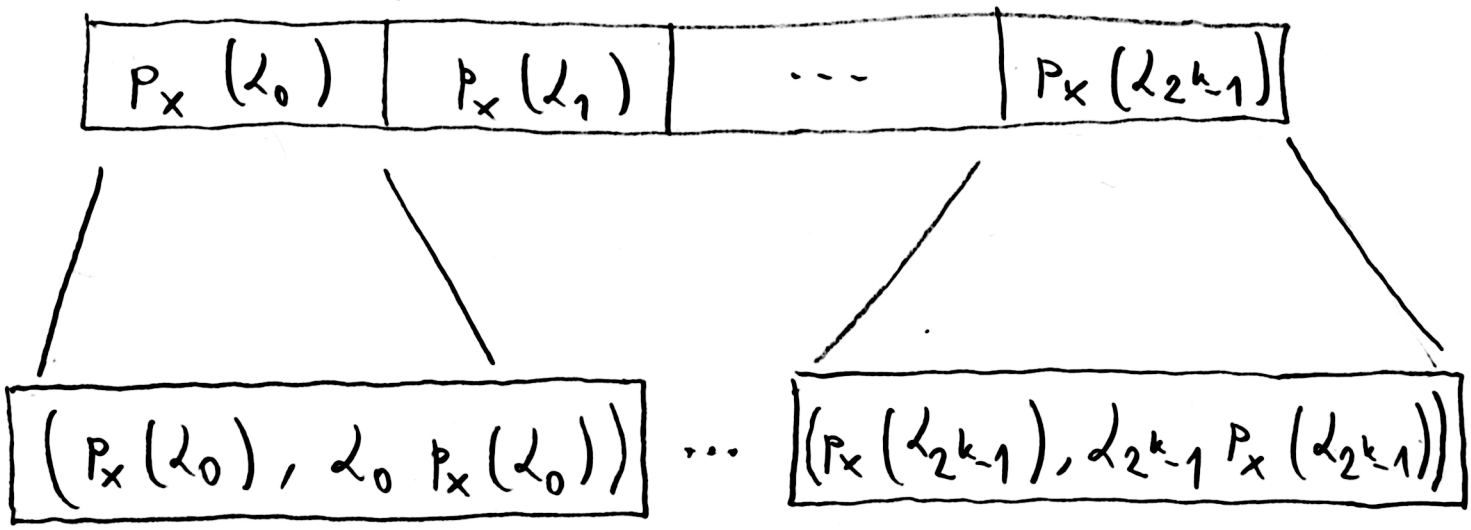
NTIN085 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI I

PRE WOZENCRAFTOV SÚBOR:

$$C_{1,\alpha_i} = \{ (x, \alpha_i x) \mid x \in GF[2^k] \}$$

$$GF[2^k] = \{ \alpha_0, \dots, \alpha_{2^k-1} \}$$

RS · WOZENCRAFT :



19.11.2010 Fr
PETER ČERNO

NTINO85 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

DEKÓDOVANIE :

$$y \longmapsto x$$

CHCEME OPRAVIŤ t CHÝB.

C MÁ MINIMÁLNU VZDIALENOSŤ $2t+1$.

→ CHCEME NÁJSŤ NAJBLIŽŠIE KÓDOVÉ SLOVO K PRIJATÉMU SLOVU

TRIVIÁLNE V ČASE: $O(q^k)$, POTR. AŽ $O(q^n)$.

PRE LINEÁRNE KÓDY ... NP TÁŽKÝ PROBLÉM

PRE y A G NÁJDI $x \in C_G$: $\Delta(x,y) = \min$.
(DOMÁCA ÚLOHA)

TOTO DEKÓDOVANIE JE "JEDNOZNAČNÉ" A FUNGUJE PO $t < \approx \frac{d}{2}$.

NIE JE MOŽNÉ OPRAVIŤ VIAC AKO $\frac{n}{2}$ CHÝB.

ZAUJÍMAVÁ OTÁZKA : CHCEME OPRAVIŤ $t = \alpha d$, $0 < \alpha < 1$.

PRE $\alpha > \frac{1}{2}$ TO JE NEJEDNOZNAČNÉ.

TÁTO OTÁZKA MÁ ZMYSEL NAPR. PRE REED-SOLOMONOVÉ KÓDY ... POČET MOŽNÝCH KANDIDÁTOV (SLOV) JE POLYNOMIÁLNY V n.

TZV. <u>LIST-DECODING</u> = DEKÓDOVANIE DO ZOZNAMU

ĎALŠIA MOŽNOSŤ (PRE VÄČŠIE ABECEDY)

VIAC MOŽNOSTÍ MÔŽU MAŤ PRAVDEPODOBNOSTI

≡ TZV. <u>SOFT-DECODING</u>

CHCEM NÁJSŤ SLOVO, KT. MAXIMALIZUJE PRAVDEPODOBNOSŤ VYSLANIA.

PRE R-S KÓDY EXISTUJÚ EF. ALGORITMY AJ PRE SOFT-DECODING.

<u>LOKÁLNE DEKÓDOVANIE</u> ... MÁME Y

PRE DANÉ $i \in \{1, \dots, k\}$ URČIŤ m_i

CHCEME VEDIEŤ SPOČÍTAŤ m_i RÝCHLO ...

... V ČASE $O(\log^{O(1)} n)$.

D. MÔŽEM SA POZRIEŤ NAJVIAC NA $O(\log^{O(1)} n)$ POZÍCIÍ ...

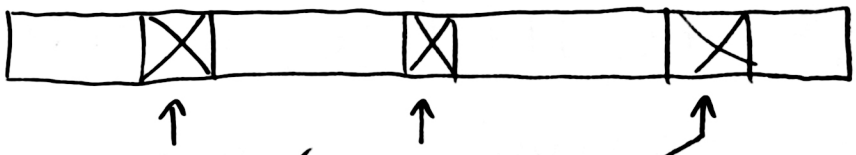
JE NUTNÉ ZAVIESŤ NÁHODNOSŤ

19.11.2010 Fr
PETER ČERNO

NTINO85 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

LINEÁRNY KÓD C

Y :



VYMAZANÉ SYMBOLY ... POZNÁME POZÍCIE
ZVYŠOK JE SPRÁVNE

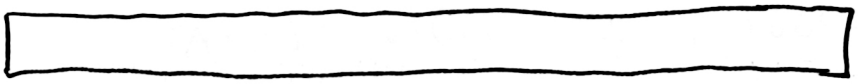
DEKÓDOVANIE :

$$m\,G = x$$

POKIAĽ TÍCH VYMAZANÝCH SYMBOLOV JE $< d$, VIEM RIEŠIŤ TÚTO ROVNICU.

LINEÁRNY KÓD $C \sim (n, k, d)_2$

Y :



HĽADÁME NAJBLIŽŠIE SLOVO

GENERUJÚCA MATICA G, KONTROLNÁ MAT. H.

$$y H = (x + e_{i_1} + \dots e_{i_t}) H =$$

$$= e_{i_1} \cdot H + \dots + e_{i_t} \cdot H$$

KEĎ $t < \frac{d-1}{2}$, POTOM Z yH VIEME URČIŤ INDEXY $i_1, \dots, i_t$.

yH SA NAZÝVA SYNDRÓM.

KEĎ $\{e_{i_1}, \dots, e_{i_t}\} \neq \{e_{i'_1} + \dots e_{i'_{t'}}\}$,

KDE $t, t' \leq \frac{d-1}{2}$,

POTOM $(e_{i_1} + \dots + e_{i_t})H \neq (e_{i'_1} + \dots + e_{i'_{t'}})H$.

AK BY BOLI ROVNAKÉ, POTOM:

$$\underbrace{(e_{i_1} + \dots + e_{i_t} - e_{i'_1} - \dots - e_{i'_{t'}})}_{t+t' \leq d-1} H = 0$$

ČO JE SPOR.

$\Rightarrow$ SYNDRÓM $y H$ JEDNOZNAČNE DEFINUJE POZÍCIE CHÝB $\{i_1, \dots, i_t\}$.

NA OPRAVOVANIE CHÝB POUŽIJEM TABUĽKU PRE $\forall$ MOŽNOSTI, KT. MÔŽU NASTAŤ.

NIEKEDY STAČÍ, KEĎ SA OBMEDZÍM NA OPRAVOVANIE MENŠIEHO POČTU CHÝB. (NAPR. ≤ 4) ... ZMENŠÍ SA TAK TABUĽKA.

DEKÓDOVANIE RS KÓDU

BERLEKAMP-WELSH '86

19.11.2010 Fr
PETER ČERNO

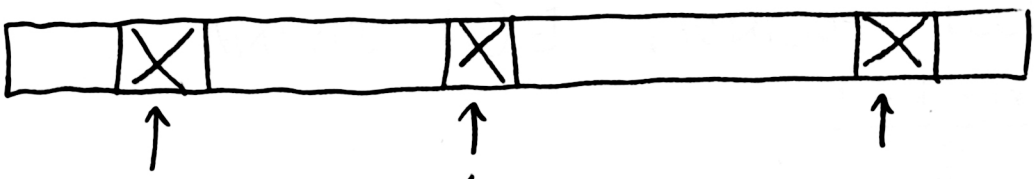
NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

P_m ... POLYNÓM STUPŇA $k-1$ NAD $GF[q]$.

$m \longmapsto (P_m(\alpha_1), \dots, P_m(\alpha_n))$

KDE $\alpha_i \in GF[q]$ SÚ NAVZÁJOM RÔZNE.

$(P_m(\alpha_1), P_m(\alpha_2), \dots, P_m(\alpha_n))$



VÝSKYTY CHÝB (POZNÁME)

INTERPOLÁCIA POLYNÓMOV:

$\beta_0, \dots, \beta_{k-1} \in GF[q]$, NAVZÁJOM RÔZNE

$\ell \in \{0, \dots, k-1\}$

EXISTUJE POLYNÓM STUPŇA $k-1$:

$$P_{\ell, \beta_0, \dots, \beta_{k-1}}(x) = \begin{cases} 0 & x \in \{\beta_0, \dots, \beta_{k-1}\} \setminus \{\beta_\ell\} \\ 1 & x = \beta_\ell \\ ? & \text{INAK} \end{cases}$$

$$P_{\ell, \beta_0, \dots, \beta_{k-1}}(x) = \frac{\prod_{i \in \{0, \dots, k-1\} \setminus \{\ell\}} (x - \beta_i)}{\prod_{i \in \{0, \dots, k-1\} \setminus \{\ell\}} (\beta_\ell - \beta_i)}$$

POVEDZME, ŽE CHCEME POLYNÓM P_m:

$P_m(\alpha_i) = r_i$ PRE k BODOV $i \in \{1, \dots, k\}$

ZREJME: $\underline{\underline{P_m(x) = \sum_{l=1}^{k} r_l \cdot P_{l, \alpha_1, \dots, \alpha_k}(x)}}$.

$\Rightarrow$ V PRÍPADE R-S KÓDOV AK POZNÁME, KDE SÚ CHYBY, NETREBA GAUSSOVU ELIMINÁCIU. STAČÍ VYŠŠIE NAZNAČENÚ INTERPOLÁCIU.

CHCEME NÁJSŤ POLYNÓM $E(x)$ STUPŇA $\leq t = \frac{n-k-1}{2}$.

BOLA VYSLANÁ SPRÁVA $(P_m(\alpha_1), \dots, P_m(\alpha_n))$

DOSTALI SME $r_1 \dots r_n$.

CHCEME, ABY:

$$E(x) = \begin{cases} 0 & \text{AK } r_i \neq P_m(\alpha_i) \ \& \ x = \alpha_i \\ ? & \text{INAK} \end{cases}$$

$E(x)$ NÁM DETEKUJE MIESTA CHÝB. PLATÍ:

PRE $\forall i$: $(r_i - P_m(\alpha_i)) E(\alpha_i) = 0$.

$$\Rightarrow \forall i: \quad r_i \underbrace{E(\alpha_i)}_{st \leq \frac{n-k-1}{2}} = \underbrace{P_m(\alpha_i) \cdot E(\alpha_i)}_{st \leq k-1 + \frac{n-k-1}{2}}$$

KOEFICIENTY: $c_0, c_1, \dots, c_{\frac{n-k-1}{2}}$

KOEFICIENTY: $c'_0, \dots, c'_{k-1+\frac{n-k-1}{2}}$

19.11.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

DOSTÁVAM:

$$r_i \cdot \sum_{j=0}^{(n-k-1)/2} c_j \alpha_i^j = \sum_{j=0}^{(n-k-1)/2+k-1} c'_j \cdot \alpha_i^j$$

POČET NEZNÁMYCH:

$$\frac{n-k-1}{2} + 1 + \frac{n-k-1}{2} + k - 1 + 1 = \underline{\underline{n}}$$

MÁM n LIN. ROVNÍC O n NEZNÁMYCH.

AKO VÝSTUP VRÁTIME:

$$\frac{P_m(x) \cdot E(x)}{E(x)} = \underline{\underline{\frac{\sum_{j=0}^{(n-k-1)/2+k-1} c'_j \cdot x^j}{\sum_{j=0}^{(n-k-1)/2} c_j x^j}}}$$

POZOR! AKO RIEŠENIE SÚSTAVY MUSÍME VZIAŤ NETRIVIÁLNE NENULOVÉ RIEŠENIE.

03.12.2010 FT
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

BERLEKAMP-WELCH ALG.

$m \in GF[q]^k \qquad p_m(x)$

$(p_m(\alpha_1), \dots, p_m(\alpha_n))$

$r_1, r_2, \dots, r_n \in GF[q]$

$\equiv$ PRIJATÁ SPRÁVA

$$E(x) = \begin{cases} 0 & \text{KEĎ } r_i \neq p_m(\alpha_i) \ \& \ x = \alpha_i \\ ? & \text{INAK} \end{cases}$$

$$\forall i \quad r_i \underbrace{E(\alpha_i)}_{\text{st.} \leq \frac{n-k-1}{2}} = \underbrace{E(\alpha_i)\, p_m(\alpha_i)}_{q(x) \quad \text{st.} \leq \frac{n-k-1}{2} + k - 1} \qquad (*)$$

TRIVIÁLNE RIEŠENIE $E(x) = 0$

ALGORITMUS: VYRIEŠIME $(*)$

PRIČOM $E(x) \neq 0$

VRÁTIME $\dfrac{q(x)}{E(x)}$.

JEDNOZNAČNOSŤ RIEŠENIA:

NECH PRE $q(x)$, $E(x)$ PLATÍ:

$$r_i E(\alpha_i) = q(\alpha_i)$$

NECH TIEŽ PRE $q'(x)$, $E'(x)$ PLATÍ:

$$r_i E'(\alpha_i) = q'(\alpha_i)$$

CHCEME UKÁZAŤ: $\dfrac{q(x)}{E(x)} = \dfrac{q'(x)}{E'(x)}$

TJ. EKVIVALENTNE: $q(x)E'(x) = q'(x)E(x)$

STUPEŇ TÝCHTO POLYNÓMOV JE $\leq n-2$.

NAVYAC SA ROVNAJÚ V n BODOCH: $\alpha_1, \dots, \alpha_n$.

$$q(\alpha_i)q'(\alpha_i) = r_i E(\alpha_i) q'(\alpha_i) = q(\alpha_i) r_i E'(\alpha_i)$$

AK $r_i \neq 0$, POTOM: $q(\alpha_i)E'(\alpha_i) = q'(\alpha_i)E(\alpha_i)$

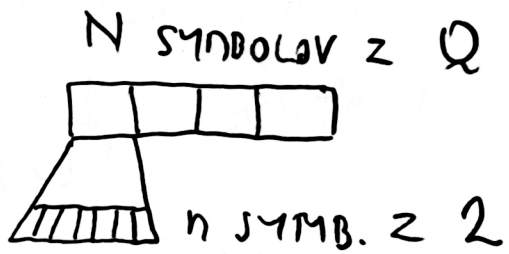
AK $r_i = 0$, POTOM: $q(\alpha_i) = q'(\alpha_i) = 0$. ■

ALGORITMUS FUNGUJE V ČASE $n \log^{O(1)} n$.

SKLADANIE KÓDOV:

$[N, K, D]_Q$, $Q = 2^k$

$[n, k, d]_2$



$\Rightarrow$ DOSTÁVAME $[N \cdot n, K \cdot k, D \cdot d]_2$

03.12.2010 Fr
PETER ČERNO

NTINOB5 VYBRANÉ KAP. Z VÝP. SLOŽITOSTI I

VEZMIME: $k = \log N$, $n = O(\log N)$, $d = \varepsilon \log N$

$2^{O(\log N)} = N^{O(1)}$

$\Rightarrow$ V POLYNOMIÁLNOM ČASE VIEME DEKÓDOVAŤ VNÚTORNÉ SYMBOLY

V ĎALŠOM KROKU DEKÓDUJ RS KÓD.

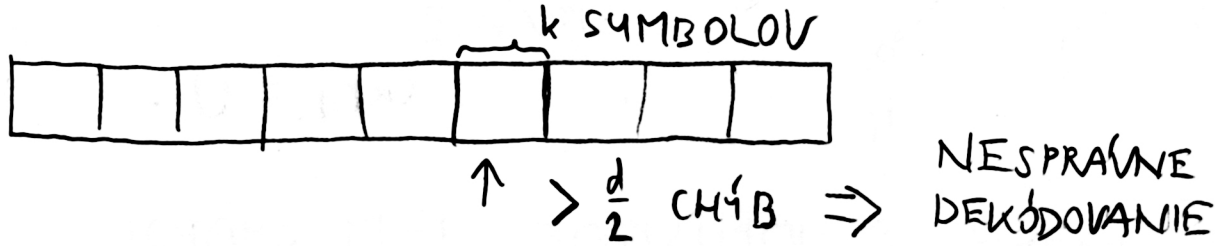
AK MÁME $> \frac{D}{2}$ CHÝB $\Rightarrow$ DEKÓDUJEME NESPRÁVNE

$\Rightarrow$ STAČÍ $\frac{D}{2} \cdot \frac{d}{2}$ CHÝB NA NESPRÁVNE DEKÓDOVANIE

CHCEME DEKÓDOVAŤ $\frac{D \cdot d}{2}$ CHÝB.

<u>OTÁZKA ZNIE</u>: AKO DEKÓDOVAŤ ZLOŽENÝ KÓD?

FORMYHO ALGORITMUS



KEĎ MÁM RS KÓD $[N, K, D]_Q$

A VYPUSTÍM s SYMBOLOV $\Rightarrow$

DOSTÁVAM RS KÓD $[N-s, K, D-s]_Q$

VIEM DEKÓDOVAŤ $\frac{D-s}{2}$ CHÝB.

CHÝB ... E

VYPUSTENÍ ... S

$$2E + S < D$$

<u>PROBLÉM</u>: NEVIEME, KT. SYMBOLY SÚ NESPRÁVNE

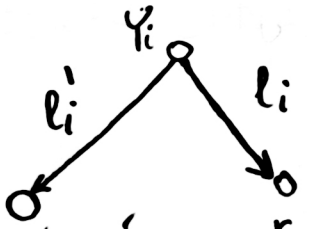
$\Rightarrow$ <u>PRAVDEPODOBNOSTNÝ ALGORITMUS</u>

1) DEKÓDUJEME VNÚTORNÉ SYMBOLY

$$\frac{r_1, r_2, \dots, r_N}{l_1, l_2, \dots, l_N}$$

... KOĽKO CHÝB SME MUSELI OPRAVIŤ

i)

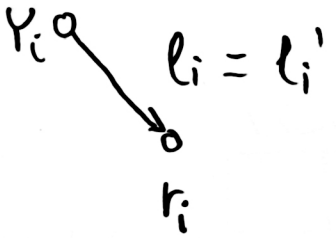


SPRÁVNE KÓDOVÉ SLOVO

AK Y DEKÓDUJEME NESPRÁVNE

NUTNE $l_i' \geq \frac{d}{2}$

ii)



AK Y DEKÓDUJEME SPRÁVNE

PRE KAŽDÉ i VYPUSTÍME i-TÝ SYMBOL S PRAVDEPODOBNOSŤOU $2l_i/d$.

ZVYŠOK DEKÓDUJEME BW ALGORITMOM.

<u>TVRDENIE</u>: $\sum l_i' < \frac{D \cdot d}{2} \Rightarrow$

$$\mathbb{E}[2E + S] < D.$$

03.12.2010 Fr
PETER ČERNO

NTINO85 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

<u>DÔKAZ.</u> PRE DANÝ i-TÝ SYMBOL:

AK ZACHOVÁM $\Rightarrow$ $E \leftarrow E+1$

AK VYPUSTÍM $\Rightarrow$ $S \leftarrow S+1$

DEFINUJME

$$E_i := \begin{cases} 1 & \text{i-TÝ SYMBOL ZACHOVÁM, A JE CHYBNE} \\ 0 & \text{i-TÝ SYMBOL VYHODÍM} \end{cases}$$

$$S_i := \begin{cases} 1 & \text{i-TÝ SYMBOL VYHODÍM} \\ 0 & \text{INAK} \end{cases}$$

(ii) $E_i = 0$

$$S_i = \begin{cases} 1 & \text{i-TÝ SYMBOL VYHODÍM} \\ 0 & \end{cases}$$

$$E = \sum_{i=1}^{N} E_i \qquad S = \sum_{i=1}^{N} S_i$$

$$\mathbb{E}[2E+S] = \mathbb{E}\left[2\sum E_i + \sum S_i\right] =$$

$$= \sum_{i=1}^{N} \mathbb{E}[2E_i + S_i]$$

(i) $\mathbb{E}[2E_i + S_i] = 2 \cdot \Pr[\text{i-TÝ S. ZACHOVÁM}]$

$+ \Pr[\text{i-TÝ S. VYHODÍM}] =$

$$= 2\left(1 - \frac{2l_i}{d}\right) + \frac{2l_i}{d} = 2 - \frac{2l_i}{d}$$

$$l_i' + l_i \geq d$$

$$l_i' \geq d - l_i$$

$$\Rightarrow \frac{2l_i'}{d} \geq 2 - \frac{2l_i}{d}$$

$$\Rightarrow \mathbb{E}[2E_i + S_i] \leq \frac{2l_i'}{d}$$

ii) $\mathbb{E}[2E_i + S_i] = 0 + 1 \cdot \Pr[\text{i-tý s. náhodný}] =$

$$= \frac{2l_i}{d} = \frac{2l_i'}{d}$$

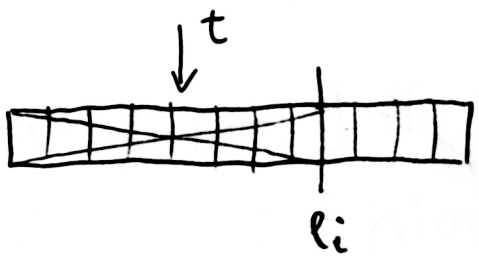
$$\Rightarrow \mathbb{E}[2E + S] \leq \sum_{i=1}^{N} \frac{2l_i'}{d} \leq \frac{2}{d} \sum_{i=1}^{N} l_i' <$$

$$< \underline{\underline{D}}. \quad \blacksquare$$

AKO SPRAVIŤ DET. ALGORITMUS:

NA ZAČIATKU NÁHODNE ZVOLÍM

$t \in \{1, \dots, \frac{d}{2}\}$



$\frac{d}{2}$

$$\frac{l_i}{\frac{d}{2}} = \underline{\underline{\frac{2l_i}{d}}}$$

NA KAŽDEJ POZÍCII TESTUJEME $t < l_i$

<u>DETERMINISTICKÁ VERZIA</u>: SKÚSIM $\forall t$. A TESTUJEM + ZAKÓDUJEM

10. 12. 2010 FT
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

KÓDY ZALOŽENÉ NA EXPANDÉROCH

- DOTERAZ ALGEBRAICKÉ KÓDY
- KOMBINATORICKÉ KÓDY – TEÓRIA GRAFOV
- STÚDIUM KONTROLNEJ MATICE $H \in \{0,1\}^{n \times m}$

$$y \in C \Leftrightarrow yH = 0$$

HAMMINGOV KÓD

$$H = \underbrace{\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 1 & 1 \\ \dots & & & & \\ 1 & 1 & \dots & 1 & 1 \end{pmatrix}}_{m = \log(n+1)} \Bigg\} n$$

$$(y + e_i)H = 0 + e_i H = i\text{-TÝ RIADOK } H$$

... UKAZUJE, KDE NASTALA CHYBA.

'63 GALLAGER

LOW DENSITY PARITY CHECK CODES.

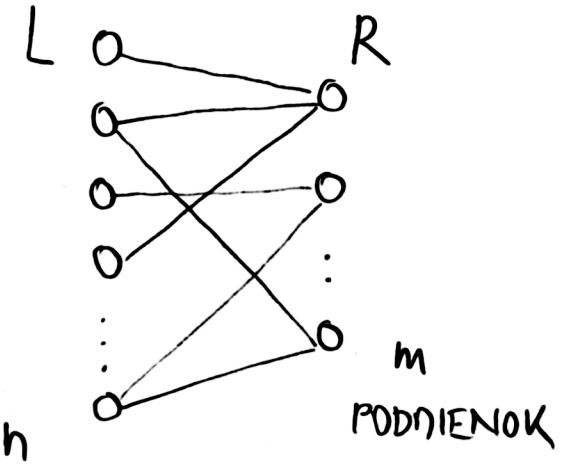
- KÓDY, V KTORÝCH KONTROLNÁ MATICA OBSAHUJE NAJVIAC l JEDNOTIEK V KAŽDOM STĹPCI ...

LDPC

GALLAGER UKÁZAL EXISTENCIU DOBRÝCH KÓDOV, KT. SÚ LDPC - DOSAHUJÚ GILBERT - VARSHAMOW MEZ.

'93 SIPSER - SPIELMAN

- VEDIA AJ DEKÓDOVAŤ
- KONTROLNÁ MATICA



BIP. GRAF

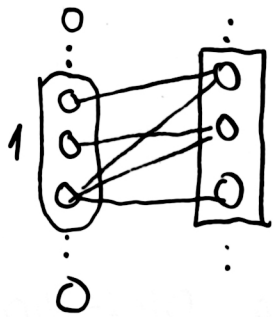
(c, ℓ) - REGULÁRNY GRAF

$\deg_L(x) = c$

$\deg_R(x) = \ell$

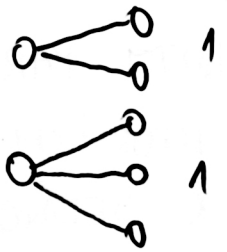
ČO CHCEME, ABY SME MALI DOBRÝ KÓD?

SLOVO S MALÝM POČTOM 1 MÁ MAŤ KÓD S MALÝM POČTOM 1



→ ASPOŇ 1 NENULOVÁ

IDEÁLNE: DISJUNKTNÍ SUSEDIA



10.12.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

DEF. : BIP., (c,ℓ)-REGULÁRNY GRAF $G=(L \dot\cup R, E)$ JE (δ, α)-EXPANDÉR

$\forall S \subseteq L: |S| \leq \delta |L| \Rightarrow |\Gamma(S)| \geq \alpha |S|$

$\Gamma(S)$ ... SUSEDIA S.

PROBLÉM: PRE $\delta = 1$, $\alpha = 1$ A $S := L$ DOSTÁVAME $|R| \geq |L|$ ...

OBMEDZUJEME SA NA ĽAVÚ STRANU.

$\Gamma_1(S)$ ... SUSEDIA S SPOJENÍ S S PRÁVE 1 HRANOU

VETA: PRE ĽUBOVOĽNÝ (δ, α)-EXPANDÉR PLATÍ, ŽE PRE $\forall S \subseteq L$, $|S| \leq \delta |L| \Rightarrow$

$|\Gamma_1(S)| \geq (2\alpha - c)|S|$.

AK $\alpha > \frac{c}{2} \Rightarrow \Gamma_1(S) \neq \emptyset$ ... A MÁME 1. :)

ABY SME DOSTALI KÓD, STAČÍ NÁJSŤ TAKÝ EXPANDÉR, O KT. UKÁŽEME, ŽE JE OK. BUDE $d = \delta n$.

C JE LINEÁRNY KÓD. BERIEME SLOVÁ $x \neq 0$ S VÁHOU $\leq \delta n$. AK PRE KAŽDÉ TAKÉTO SLOVO x BUDE ASPOŇ 1 PARITA $= 1$ ... MÁME KOREKTNÝ EXPANDÉR.

GRAFY SA ŤAŽKO HĽADAJÚ!

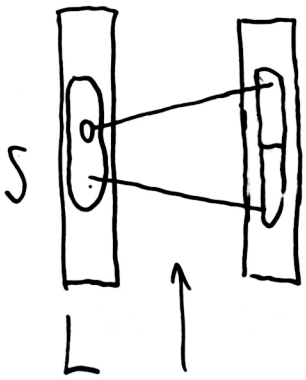
2002 – VIEME EXPLICITNÚ KONŠTRUKCIU (CAPALBO, REINGOLD, ...)

$\alpha > (1-\varepsilon)c$ ... NÁJDEM EXPANDÉR

NÁHODNÝ GRAF JE $(\delta, c-1)$ - EXPANDÉR

MALÉ MNOŽINY ... EXPANDUJÚ

<u>DÔKAZ TVRDENIA</u>. MAJME (δ, α) - EXPANDÉR



$U = \Gamma_1(S)$

$D = \Gamma(S) - \Gamma_1(S)$

$|\Gamma(S)| \geq \alpha |S|$

$c|S|$ HRÁN DO $\Gamma(S)$

(1) $c|S| \geq |U| + 2|D|$

PRÁVE 1 HRANA ASPOŇ 2 HRANY

(2) $|U| + |D| = |\Gamma(S)| \geq \alpha |S|$

$\Rightarrow 2|U| \geq 2\alpha|S| - 2|D|$

(1) + (2) : $c|S| + 2|U| \geq |U| + 2\alpha|S|$

$\Rightarrow |U| \geq (2\alpha - c)|S|$. $\square$

10.12.2010 Fr
PETER ČERNO

NTINO85 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

CHCEME DOBRÝ DEKÓDOVACÍ ALGORITMUS
... KÓDOVANIE JE JASNÉ

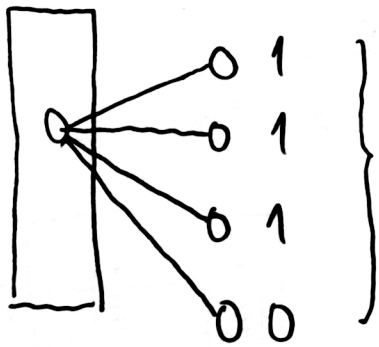
DEKÓDOVANIE :

OPRAVUJE TOĽKO CHÝB
↓

$\frac{\delta}{2}n$ BY SME CHCELI ... DOSTANEME $\varepsilon n \leq \frac{\delta}{2c} n$

OPAKUJ, KÝM SA DÁ:

VYBER VRCHOL VĽAVO, PRE KTORÝ VÄČŠINA PARÍT NIE JE SPLNENÁ A NEGUJ PRÍSLUŠNÝ BIT (=1)



VÄČŠINA ZLE ⇒ PREHOĎ

VETA : AK POČET CHÝB JE < AKO $\frac{\delta}{2c} n$, $\lambda > \frac{3}{4} c$, POTOM SA ALG. ZASTAVÍ SO SPRÁVNYM KÓDOVÝM SLOVOM PO NAJVIAC $\frac{\delta}{2} n$ KROKOCH.

- PO PREHODENÍ SA ZNÍŽI POČET 1 VPRAVO
- NA ZAČIATKU JE VPRAVO NAJVIAC $\frac{\delta}{2} n$ 1.
  $\left(\frac{\delta}{2c} n \cdot c = \frac{\delta}{2} n \right)$ ⇒ NAJVIAC $\frac{\delta}{2} n$ KROKOV. ✓
- ZOSTÁVA OVERIŤ KOREKTNOSŤ.

CHCEME UKÁZAŤ, ŽE NÁJDEME KÓDOVE SLOVO (VPRAVO SAMÉ 0 ...)

ALGORITMUS SA ZASEKNE, AK VPRAVO EXISTUJE 1 A NEMÁME VHODNÝ VRCHOL.

UKÁŽEME, ŽE TO NENASTANE ...

NAVIAC UKÁŽEME, ŽE NÁJDEME SPRÁVNE SLOVO -

a) PRIJATÝ VEKTOR SA VZDIALI OD PÔVODNÉHO O NAJVIAC $\delta/2\, n$.

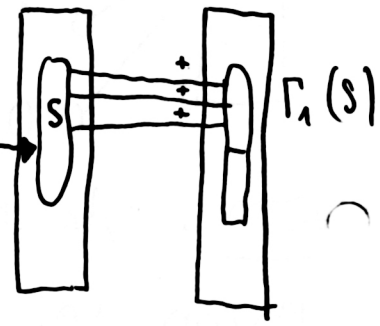
εn CHÝB SOM MAL. $\varepsilon n + \frac{\delta}{2} n < \delta n$ ✓

(# ZMIEN OPROTI KÓD. SLOVU)

$\Rightarrow$ SKONČÍM NA POŽADOVANOM SLOVE.

b) NEZASEKNEM SA. POUŽI $\alpha > \frac{3}{4} c$ A TVRDENIE:

$$|\Gamma_1(S)| \geq (2\alpha - c)|S| > \frac{|S|c}{2}.$$



AKTUÁLNY OBJEM CHÝB V SLOVE: S

$$|S| \leq \frac{\delta}{2} n + \varepsilon n < \delta n$$

MÁ ASPOŇ $\frac{|S|c}{2}$ JEDNOZNAČNÝCH SUSEDOV

MÁME: $Y + e_S$

$Y \in C$

BITY Y PRISPIEVAJÚ DO PARÍT NULAMI

JE TO TO ISTÉ, AKO KEBY SOM UVAŽOVAL IBA e_S.

PARITY VPRAVO ZODPOVEDAJÚ e_S.

10.12.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

$\Gamma_1(S)$ ... TO SÚ TIE, ČO MAJÚ CHYBU.
SÚ NASTAVENÉ NA 1. OPRAVA V e_S ICH DÁ NA 0.

$|\Gamma_1(S)| > \frac{c}{2}|S| \Rightarrow \exists x \in S$, PRE KTORÉ VÄČŠINA SUSEDOV MÁ 1,
PRETOŽE VIAC AKO $\frac{c}{2}|S|$ HRÁN MÁ 1.
(TJ. VIAC AKO POLOVICA ...)

LINEÁRNY ČAS

- AK MÁM GRAF ...
- KÓDOVANIE JE JASNÉ:
  VYRIEŠ $y H = 0 \Rightarrow$ DOSTANEŠ GEN. MATICU G

NÚ: $\alpha \geq c \Rightarrow$ VIEM OPRAVIŤ AŽ $\frac{\delta}{2} n$ CHÝB TÝMTO ALGORITMOM?

PROBLÉM S KONŠTRUOVATEĽNOSŤOU

'93 ... INÉ KÓDY S MALOU EXPANZIOU
STAČILO $\alpha \neq 0$ (A) $\alpha < \frac{c}{2}$)
KONŠTRUKCIA EXPANDÉROV UŽ BOLA ZNÁMA
EXPANDÉRY:
- ANALÓGIA S VL. ČÍSLAMI MATICE,
- NAJLEPŠIE EXPANDÉRY ... $\alpha \approx \frac{c}{2}$.

'93 KÓDY + GALLAGER IMPROVED

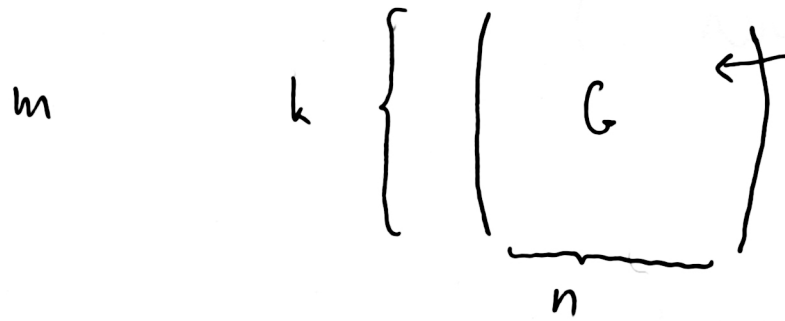
SIPSER - SPIELMAN

- ROZVÍJA EXPANDÉRY, ALE NIE RIEDKA MATICA
... ZLOŽITEJŠIA KONSTRUKCIA

→ NOVÉ KÓDY, LINEÁRNE, ENCODE, DECODE : $O(n)$

H, G RIEDKA ... NEFUNGUJE

G RIEDKA ⇒ $x G$ MÁ MÁLO 1 ... MALÉ VZDIAL.



$O(n)$ JEDNOTIEK

$k = \varepsilon n$

⇒ V RIADKU KONŠT. VEĽA 1.

ZMENA 1 BITU V SPRÁVE ZMENÍ KONŠT. VEĽA 1-TIEK V KÓDOVOM SLOVE ⇒ ZLÝ KÓD, MYSLIENKA DOBRÁ.

17.12.2010 Fr
PETER ČERNO

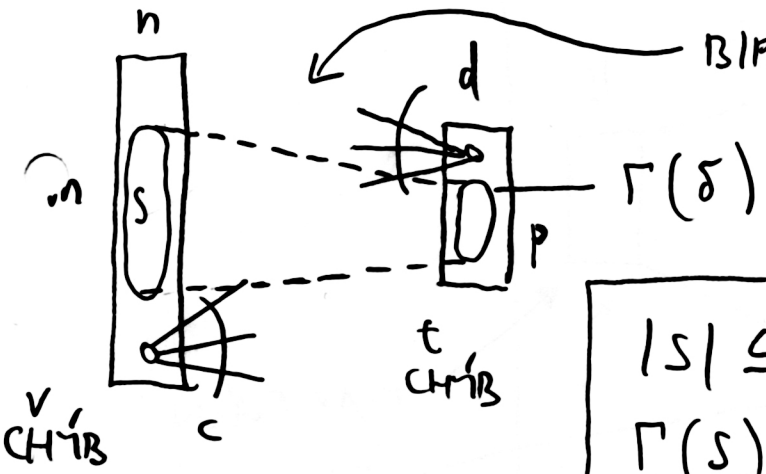
NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

SIPSER - SPIELMAN
SPIELMAN '96

POPÍSAŤ POZNÁMKY Z 10.12.2010

(c, ℓ) - REGULÁRNY (δ, γ) - EXPANDER

BIPARTITNÝ GRAF



$$|S| \leq \delta n \Rightarrow \Gamma(S) > \gamma |S|$$

SUSEDIA MN. S

DEKÓDOVANIE ... $O(n)$

$m \xrightarrow[\text{KÓD}]{} (m, p)$

$$G = \begin{pmatrix} 1 & & 0 & \\ & 1 & & \\ 0 & & \ddots & 1 \end{pmatrix}$$

RIEDKA MATICA

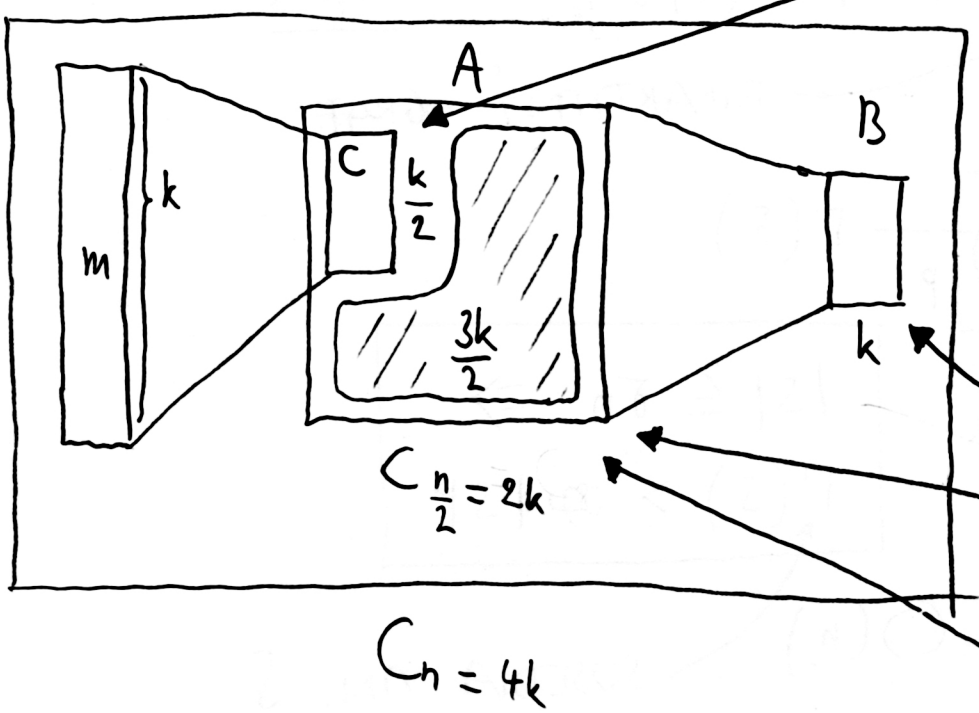
REKURZÍVNE KÓDOVANIE

$$(m, \underbrace{p(m), p(p(m)), \ldots}_{\log m})$$

ERROR REDUCTION CODE

$k \longrightarrow 4k = n$

OPRAVÍ $\frac{\delta}{4} n$ CHÝB



PO KROKU (2) BEZCHYBNÉ C

MAXIMÁLNE δk CHÝB

$\Rightarrow$ PO KROKU (1) $\frac{\delta}{2} k$ CHÝB $= \frac{\delta}{4} \frac{n}{2}$

(PRE $n = n_0$ POUŽIJEM C_{n_0} VYTVORENÝ HRUBOU SILOU)

$$\boxed{\text{AK } v, t \leq \frac{\delta}{4} n \Rightarrow \text{POČET CHÝB } v' \leq \frac{t}{2}.}$$

DEKÓDOVANIE:

(1) POMOCOU B ZNÍŽ POČET CHÝB V A

(2) DEKÓDUJ C Z A

(3) DEKÓDUJ / ZNÍŽ POČET CHÝB V PÔVODNEJ SPRÁVE m POMOCOU C.

ČAS. ZLOŽ.: $D(n) \leq \underset{(1) + (3)}{O(n)} + \underset{(2)}{D(\frac{n}{2})}$

17.12.2010 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAPITOLY Z VÝP. SLOŽITOSTI I

ERROR REDUCTION ALGORITHUS

- PRE KAŽDÝ BIT SPRÁVY SPOČÍTAJ POČET NESPLNENÝCH SUSEDOV (PARITNÝCH BITOV)
- AK PRE NIEKTORÝ BIT SPRÁVY JE POČET NESPLNENÝCH SUSEDOV $> c/2$, POTOM TENTO BIT ZNEGUJ.
- OPAKUJ DOKEDY TAKÝ BIT EXISTUJE.

$l = 2c$, TJ. $(c, 2c)$-REGULÁRNY EXPANDÉR S PARAMETRAMI $(\alpha, \frac{3}{4}c + 2)$, KDE $\delta = \frac{\alpha}{2}$.

V = NESPRÁVNE BITY V SPRÁVE m

T = NESPRÁVNE BITY V PARITÁCH p

$v = |V|$, $t = |T|$, $|m| = k$, $|p| = \frac{k}{2}$

u ... POČET NESPLNENÝCH PARITNÝCH BITOV

s ... POČET SPLNENÝCH PARITNÝCH BITOV SO SUSEDOM VO V.

V SA MENÍ, T SA NEMENÍ, u, s SA MENIA

CHCEME UKÁZAŤ, ŽE KEĎ SA TEN ALGORITMUS ZASTAVÍ, POTOM $v' \leq \frac{t}{2}$.

PLATÍ: $\alpha k \geq v \geq \frac{t}{2} \Rightarrow$

(i) $u + s > \left(\frac{3}{4}c + 2\right)v$

VYPLÝVA Z TOHO, ŽE MÁME $(\alpha, \frac{3}{4}c+2)$-EXP.

(ii) $cv + t \geq u + 2s$

NESPRÁVNE PARITNÉ BITY

HRÁN, KT. VYCHÁDZAJÚ Z NESPRÁVNYCH BITOV SPRÁV

PARITNÝ BIT, KT. JE NESPLNENÝ A JE SPRÁVNE $\rightarrow$ MÁ SUSEDA VO V

TRIVIÁLNE: $cv + t \geq u$

TAKTIEŽ $cv + t \geq 2s$

PRI ROZBORE PRÍPADOV TÝCHTO NEROVNOSTÍ SME PARITNÝM BITOM PRIRADZOVALI VŽDY DISJUNKTNÉ VEĽCI ... TJ. $cv + t \geq 2s + u$

DÔSLEDOK:

$s < \left(\frac{c}{4} - 2\right)v + t$ ... (ii) − (i)

$u > \left(\frac{c}{2} + 4\right)v - t$ ... 2(i) − (ii)

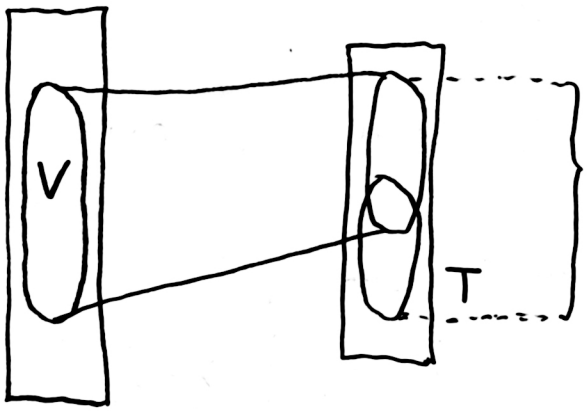
POUŽITÍM PREDPOKLADU $\alpha k \geq v \geq \frac{t}{2}$:

$u > \frac{c}{2}v + t$

$\Rightarrow$ POČET NESPLNENÝCH SUSEDOV V JE $> \frac{c}{2}v$.

17.12.2010 Fr
PETER ČERNO

NTINO85 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI I



OBSAHUJÚ I VŠETKY NESPLNENÉ VRCHOLY

ZOSTÁVA UKÁZAŤ, ŽE v NEMÔŽE DOSIAHNUŤ αk.
PRE SPOR, NECH $v = \alpha k$.
NA ZAČIATKU $v \leq \frac{\alpha k}{2}$, $u \leq cv + t \leq \frac{c\alpha}{2}k + \frac{\alpha}{2}k$
$u \searrow 0$ KLESÁ.
Z $u > \left(\frac{c}{2} + 4\right) v - t$ DOSTÁVAME

$$u > \left(\frac{c}{2} + 4\right)\alpha k - t$$

$t \leq \delta k$, TAKŽE: $u > \left(\frac{c}{2}+4\right)\alpha k - \frac{\alpha k}{2} =$

$$= \underline{\underline{\frac{c\alpha}{2}k + \frac{7}{2}\alpha k}},$$ ČO JE SPOR ↯.

PODOBNE PRE $\alpha k - c < v \leq \alpha k$.

07. 01. 2011 Fr
PETER ČERNO

NTINDB5 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI I

LOKÁLNE DEKÓDOVATEĽNÉ KÓDY

$i \in \{1, \dots, k\}$ $\longrightarrow$ m_i

KLASICKÉ DEKÓDOVANIE ... ČAS $poly(n, k)$

LOKÁLNE DEKÓDOVANIE ... CIEĽ:

$poly(\ell, \log n)$

m_i ODVODÍME Z ℓ MIEST.

DEKÓDOVANIE ... PRAVDEPODOBNOSTNÉ

KÓD $C \subseteq \Sigma^n$ JE ℓ-LOKÁLNE DEKÓDOVATEĽNÝ Z δn CHÝB, KEĎ EXISTUJE PRAVD. ALGORITMUS A PRACUJÚCI V ČASE $poly(\ell, \log n)$, KTORÝ NA VSTUPE i A S PRIAMYM PRÍSTUPOM K $r \in \Sigma^n$, KDE $\exists! w_m \in C : \Delta(w_m, r) \leq \delta n$, VYDÁ m_i S PRAVDEPODOBNOSTOU $\geq \frac{2}{3}$, POUŽITÍM ℓ DOTAZOV K r.

$m \xmapsto{C} w_m$

PRÍKLAD: RS KÓD $[n, k, n-k+1]_n$ NIE JE $(k-1)$-LOKÁLNE DEKÓDOVATEĽNÝ

PRÍKLAD: HADAMARDOV KÓD $[n, k, \frac{n}{2}]_2$

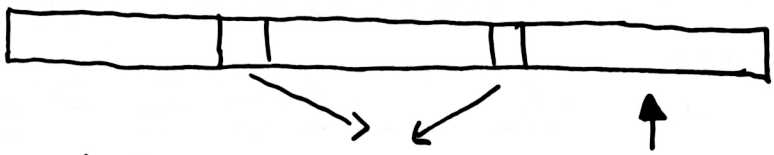
$a_1, \dots, a_k \in GF[2]$

$p_{a_1, \dots, a_k}(x_1, \dots, x_k) = \sum_{i=1}^{k} a_i x_i$

$\bar{a} \mapsto (p_{\bar{a}}(00\dots0), p_{\bar{a}}(00\dots1), \dots, p_{\bar{a}}(11\dots1))$

VETA: HADAMARDOV KÓD JE 2-LOK. DEKÓDOVATEĽNÝ AŽ PRE $\delta = \frac{1}{6}$.

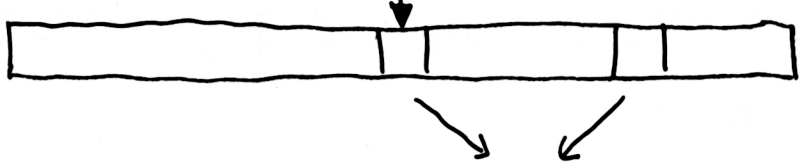
$\bar{a} \mapsto$



$i \in \{1, \dots, k\}$ $\quad a_i \quad$ 1/6 CHYB

AKO ZVOLIŤ $\ell = 2$ MIESTA:

ZVOLÍM NÁHODNE y $\quad y + e_i$



$r_y + r_{y+e_i}$

07.01.2011 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI I

r_y JE NESPRÁVNE S PRAVD. $\leq \frac{1}{6}$

PODOBNE r_{y+e_i}

VÝSLEDOK $r_y + r_{y+e_i}$ JE SPRÁVNE, KEĎ SÚ OBE r_y, r_{y+e_i} SPRÁVNE / NESPRÁVNE, TJ. S PRAVD. ASPOŇ $\frac{2}{3}$.

EXISTUJE 3-LOK. KÓD S $n = 2^{k^{O(1)}}$ ...

<u>OTVORENÝ PROBLÉM</u>: c-LOK. KÓD S $n = k^{O(1)}$

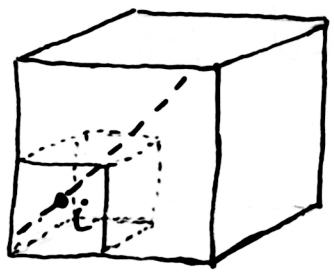
<u>REED-MÜLLEROVE KÓDY</u> NAD $GF[q]$, $q < n$

$$P_m(x_1, \dots, x_s) = \sum_{j_1 + \dots j_s < D} m_{j_1, \dots, j_s} x_1^{j_1} \dots x_s^{j_s}.$$

$m \longmapsto$

$$\left(P_m(\alpha_1^1, \dots, \alpha_s^1), \dots, P_m(\alpha_1^n, \dots, \alpha_s^n) \right)$$

$\alpha_1^i, \dots, \alpha_s^i \in GF[q] \quad \forall i.$ <u>DUÁLNA</u> VERZIA:



$GF[q]^3$

SPRÁVA m BUDE DEF. HODNOTY P_m V k BODOCH ...

$\vec{\alpha}^i \in GF[q]^3$, ZVOLÍME $\vec{\beta} \in GF[q]^3$.

UVAŽUJME PRIAMKU

$$\ell(t) = \{ \vec{\alpha}^i + t \cdot \vec{\beta} \mid t \in GF[q] \}$$

$$P_m(\alpha_1^i + t \cdot \beta_1,\ \alpha_2^i + t \cdot \beta_2,\ \alpha_3^i + t \cdot \beta_3)$$

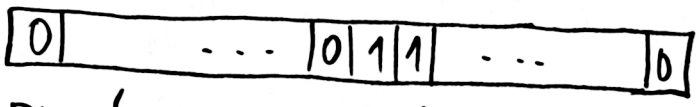
JE POLYNÓM V t STUPŇA $< D$.

KEĎ ZAFIXUJEM t A BERIEM β NÁHODNE
... DOSTANEM ROVNOMERNE ROZDELENÉ BODY

<u>POUŽITIE LOK. DEKÓDOVANIA:</u>

- INTERAKTÍVNE PROTOKOLY
- V KRYPTOGRAFII: PRIVATE INFORMATION RETRIEVAL (PIR)

$\Sigma^{30} = Q$



DLHÝ REŤAZEC $|Q|$

ZAUJÍMA NÁS 1 BIT

AKO STIAHNUŤ DATA Z DB BEZ TOHO, ABY SME DB POVEDALI, ČO CHCEME ...

TRIVIÁLNY PRÍSTUP: DAJ MI CELÚ DB

07.01.2011 Fr
PETER ČERNO

NTIN085 VYBRANÉ KAP. Z VÝPOČETNÍ SLOŽITOSTI I

UVAŽUJME DVA VYHĽADÁVAČE: GOOGLE, BING

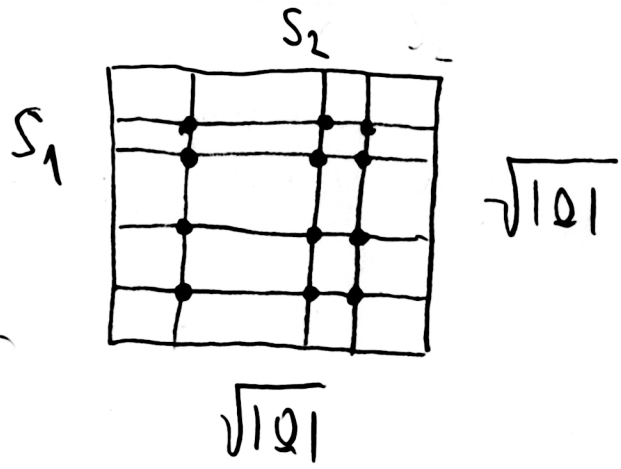
VEZMEME $S \subseteq Q$ (MASKA) ... NÁHODNE

GOOGLU POŠLEME DOTAZ S

BINGU POŠLEME DOTAZ $S \Delta \{i\}$

ANI GOOGLE, ANI BING NEVIEDIA, ČO NÁS ZAUJÍMA, A ZÁROVEŇ NIEMA DEKÓDOVAŤ i-TÝ BIT.

INÝ PRÍSTUP:



BING/GOOGLE ODPOVIE: SÚČET V PRIESEČNÍKU S_1 & S_2.

POLOŽÍME DOTAZ: (S_1, S_2), DOSTANEME:

$(S_1 \Delta \{j\}, S_2)$

$(S_1, S_2 \Delta \{j\})$ $\quad \forall j \in \{1, \dots, \sqrt{n}\}$

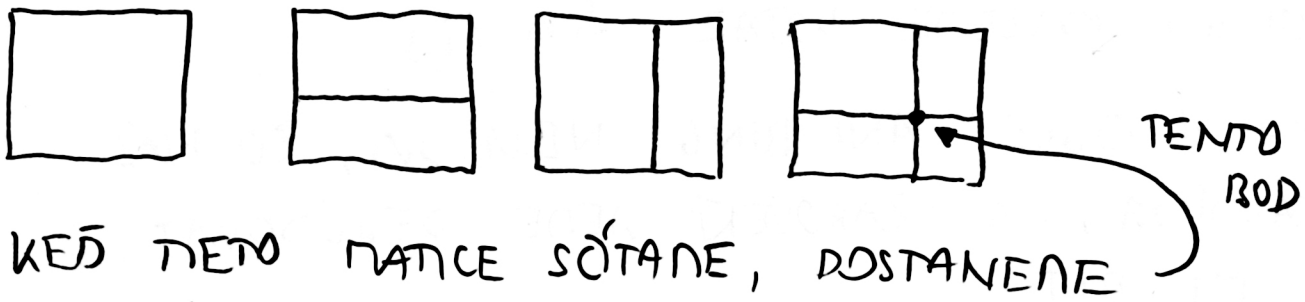
CELKOVÝ OBJEM PRENESENÝCH DÁT NA OBOCH STRANÁCH JE $2\sqrt{n}$.

PROTOKOL:

ZVOLÍME $S_1, S_2 \subseteq \{1, \dots, \sqrt{n}\}$ NÁHODNE

GOOGLE DOSTANE DOTAZ (S_1, S_2)

BING DOSTANE DOTAZ $(S_1 \Delta \{i_r\}, S_2)$



KEĎ TIETO MATICE SČÍTAME, DOSTANEME (JEDINÝ BOD, KT. SA VYSKYTUJE V TOMTO SÚČTE NEPÁRNY POČET KRÁT)